

The COAST GUARD Journal of Safety
& Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council

Winter 2014–2015

Cybersecurity

- *Vulnerabilities*
- *Threats*
- *Risk Management*

| Report Documentation Page | | | | Form Approved OMB No. 0704-0188 | |
|--|------------------------------------|-------------------------------------|---|---|---------------------------------|
| Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. | | | | | |
| 1. REPORT DATE 2015 | | 2. REPORT TYPE | | 3. DATES COVERED 00-00-2015 to 00-00-2015 | |
| 4. TITLE AND SUBTITLE Coast Guard Proceedings. Volume 71, Number 4, Winter 2014-2015 | | | | 5a. CONTRACT NUMBER | |
| | | | | 5b. GRANT NUMBER | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | |
| 6. AUTHOR(S) | | | | 5d. PROJECT NUMBER | |
| | | | | 5e. TASK NUMBER | |
| | | | | 5f. WORK UNIT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Coast Guard, 2100 2nd Street SW Stop 7681, Washington, DC, 20593-7681 | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | |
| 14. ABSTRACT | | | | | |
| 15. SUBJECT TERMS | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT Same as Report (SAR) | 18. NUMBER OF PAGES 92 | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT unclassified | b. ABSTRACT unclassified | c. THIS PAGE unclassified | | | |

PROCEEDINGS



Winter 2014–2015

Vol. 71, Number 4

Governance

- 6 **Maritime Governance:** Designed with security in mind.
by Ms. Danielle Bivens
- 8 **The Coast Guard and Cybersecurity:** A legal framework for prevention and response.
by LCDR Brandy Parker and Mr. Glenn Gray
- 12 **C-Cubed:** Increasing cyber resilience, awareness, and managing risk.
by Mr. Thad Odderstol
- 15 **Reducing Cyber Risk:** Marine transportation system cybersecurity standards, liability protection, and cyber insurance.
by Mr. David Dickman, Mr. Dismas N. Locaria, and Mr. Jason Wool
- 18 **Cyberspace—the Imminent Operational Domain:** A construct to tackle the Coast Guard's tough challenges.
by CAPT Jeff Radgowski and CAPT Katherine Tiongson

Information Systems

- 22 **Shifting the Paradigm:** The DHS Continuous Diagnostics and Mitigation Program.
by Mr. Eric Goldstein and Mr. Mark Kneidinger
- 25 **Hacking 101:** Using social engineering increases security attack effectiveness.
by Mr. Ron Schnell
- 28 **Zero-Day Vulnerabilities:** What to do when it's too late to prevent an attack.
Prof. Xiuwen Liu, Prof. Mike Burmester, Mr. W. Owen Redwood, Mr. Fred Wilder, Captain USCG (ret.), and Mr. Judd Butler
- 34 **Securing Your Control Systems:** Overcoming vulnerabilities.
by Mr. Mate J. Csorba, Ph.D. and Mr. Nicolai Husteli

Cybersecurity of Maritime Critical Infrastructure

- 38 **Building Port Resilience:** How cyber attacks can affect critical infrastructure.
by Ms. April Danos
- 42 **Maritime Critical Infrastructure Cyber Risk:** Threats, vulnerabilities, and consequences.
by LCDR Marshall E. Newberry
- 45 **Control System Cybersecurity:** Legacy systems are vulnerable to modern-day attacks.
by LCDR Jennifer M. Konon
- 48 **Hide and Seek:** Managing Automatic Identification System vulnerabilities.
by LCDR Allison Middleton
- 50 **GPS Spoofing and Jamming:** A global concern for all vessels.
by Ms. Brittany M. Thompson

Information Sharing and Intelligence

- 52 **Department of Homeland Security Efforts:** Implementing cybersecurity initiatives throughout the federal government.
by LCDR Maureen D. Johnson
- 55 **Countering the Maritime Cyber Threat:** The FBI's expanding partnerships and programs.
by Supervisory Special Agent Richard Kolko
- 62 **Rethinking Reporting:** Handling transportation cybersecurity incidents.
by Mr. Weston R. Laabs
- 65 **Cyber Intelligence Operations:** More than just ones and zeroes.
by Mr. Randy Borum, Ph.D., Mr. John Felker, Captain USCG (ret.), and Lieutenant Colonel Sean Kern, USAF

Insider Threat

- 69 **Combating Insider Threat:** The greatest threats are the ones with access.
by Mr. Greg Smith
- 72 **The Threat Within:** Protecting against internal enemies.
by Mr. Scott O'Connell
- 77 **The Frenemy:** Insider threats in the maritime environment.
by Colonel Steve Coppinger (USAF, ret.)

Lessons Learned

- 81 **Into the Storm:** Tall ship *Bounty* founders at sea.
by Ms. Sarah K. Webster

Deck

- | | | | |
|---|--|----|--|
| 4 | Assistant Commandants' Perspective <i>by Rear Admiral Marshal B. Lytle III and Rear Admiral Paul F. Thomas</i> | 91 | Upcoming in Proceedings |
| 5 | Champion's Point of View <i>by CAPT Michael C. Dickey</i> | 86 | Chemical of the Quarter Understanding Dimethyl Sulfide <i>by Cadet Nickolette Morin</i> |
| | | | Nautical Queries |
| | | 87 | Engineering |
| | | 89 | Deck |

Cover image by bestdesigns/iStock/Thinkstock.
Graphics USCG and its licensors, unless otherwise indicated.

Admiral Paul F. Zukunft
Commandant
U.S. Coast Guard

**The Marine Safety
& Security Council
of the
United States Coast Guard**

Rear Admiral Steven D. Poulin
Judge Advocate General
Chairman

Mr. Jeffrey G. Lantz
Director of Commercial
Regulations and Standards
Member

Rear Admiral Peter J. Brown
Assistant Commandant
for Response Policy
Member

Rear Admiral Paul F. Thomas
Assistant Commandant
for Prevention Policy
Member

Rear Admiral Todd A. Sokalzuk
Assistant Commandant for
Resources, Chief Financial Officer
Member

Rear Admiral Peter W. Gautier
Director for Governmental
and Public Affairs
Member

Captain Jonathan C. Burton
Director of Inspections
and Compliance
Member

Mr. William R. Grawe (Acting)
Director of National Pollution
Funds Center
Member

Mr. Gary C. Rasicot
Director of Marine Transportation
Systems Management
Member

Ms. Mary E. Landry
Director of Incident Management
and Preparedness Policy
Member

Mr. Michael W. Mumbach
Executive Secretary



Assistant Commandants' Perspective



By REAR ADMIRAL MARSHALL B. LYTLE III
*Acting Deputy Commandant for Mission Support
Assistant Commandant for Command, Control,
Communications, Computers, and
Information Technology
Commander, U.S. Coast Guard Cyber Command*

&

REAR ADMIRAL PAUL F. THOMAS
*Assistant Commandant for
Prevention Policy
U.S. Coast Guard*

Since its founding in 1790, the Coast Guard has long defended our nation from all manner of maritime threats. Piracy, smuggling, and disasters on the sea were the stocks-in-trade for Alexander Hamilton's Revenue Cutters, as they are for today's modern Coast Guard.

Those early sailors understood the meaning of seamanship, and the service eventually incorporated commercial vessel and facility inspection activities, establishing a tie with the marine industry that is foundational to our modern maritime safety and security programs. From missions involving boiler explosions and fires to oil spills, natural disasters, and terrorist attacks, we have achieved a remarkable degree of success in reducing risk and protecting the American people and the vessels, facilities, crews, and workers that make up the marine transportation system, from all hazards and threats.

Cybersecurity represents the latest risk to this system and is a growing concern for consumers, corporations, and law enforcement agencies. This concern is well founded. Computers and other cyber-dependent technologies are growing parts of our lives and businesses. These systems are potentially vulnerable to many types of risks, from deliberate attacks, to the unintended but damaging introduction of malware, to simple technical failure.

In most cases, cyber "accidents" are at least as likely as a targeted cyber attack. Regardless of the source or motivation of the threat, however, cyber vulnerabilities within the marine transportation system could compromise vital safety, security, and environmental functions, or lead to widespread trade disruptions.

While cybersecurity risks are real and growing, so is our commitment to address them. The Coast Guard is developing policies to help industry address cybersecurity in a systematic way. We are also taking measures to protect our own systems and to address cybersecurity at the port level through area maritime security committees.

This edition of *Proceedings* includes a wealth of information that can help the marine industry understand and address this risk. In particular, we encourage industry to review the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, and the associated Critical Infrastructure Cyber Community Voluntary Program developed by the Department of Homeland Security.

Social engineering and zero-day vulnerabilities must now become as much a part of our vocabulary as relief valves and fire drills. We thank the authors for their work in developing such a rich collection of information that can help us all develop a "culture of cybersecurity."

Champion's Point of View



by CAPT MICHAEL C. DICKEY
Deputy Commander
U.S. Coast Guard Cyber Command

While this edition of *Proceedings* focuses on cybersecurity, it is not the only recent edition focused on security challenges. Previous edition topics include: maritime domain awareness, enhancing global supply chain security, and maritime border security. Each explored the concerns and security risks associated with the physical domain and the need to develop a marine activity common situational picture to improve safety and security. As this edition of *Proceedings* adds to that discussion, so, too, does cybersecurity add to the Coast Guard's overall efforts to address the many safety and security challenges in the maritime domain.

It is apparent from the variety of articles that cybersecurity is a complex topic. While on the surface, cyberspace appears to be mostly a technical domain that requires technical solutions to secure it, a quick perusal of the articles in this issue makes it very clear that technical solutions are only part of the answer.

The first section is made up of articles that address governance issues surrounding maritime transportation system cybersecurity. Included in the next section is an article by Mr. Ron Schnell that addresses a decidedly non-technical approach that is a favorite tool of many accomplished hackers—social engineering.

The title of this issue lists three aspects of cybersecurity: vulnerabilities, threats, and risk management. With the exception of extremely specialized systems, we all are faced with the same sets of vulnerabilities, because we all use systems that are dependent on a few different operating systems and essential applications. Likewise, the threats we face are similar. The article by LCDR Marshall Newberry on maritime critical infrastructure cyber risk describes some threat categories that apply across industry and government.

Additionally, due to global supply chain interconnectivity, moving people, cargo, and vessels efficiently and securely relies on a regular information exchange between government and industry. Several articles in this issue address the importance of information sharing and intelligence.

Finally, we have devoted a section to the insider threat, which is a real problem for public and private sector organizations. Managing risk is where each service provider organization must apply inside knowledge regarding critical business processes and the systems those processes depend on. It will never be possible for us to create a completely secure information technology system, so we must all apply shared knowledge of vulnerabilities and threats and our internal knowledge of the systems we are responsible for to manage limited resources to minimize overall risk to our organizations.

It is critical that we work together to share information about cyber activities within the maritime domain to ensure our electronic borders are secure from bad cyber actors, and to enable efficient and effective global supply chain operation.

Editorial Team

Barbara Chiarizia
Executive Editor

Leslie C. Goodwin
Art Director

Sarah K. Webster
Managing Editor

Proceedings is published quarterly in the interest of safety at sea under the auspices of the Marine Safety & Security Council. Special permission for republication, either in whole or in part, except for copyrighted material, is not required, provided credit is given to *Proceedings*.

The articles contained in *Proceedings* are submitted by diverse public and private interests in the maritime community as a means to promote maritime safety and security. The views expressed by the authors do not necessarily represent those of the U.S. Coast Guard or the Department of Homeland Security or represent official policy.

Editorial Contact

Email: HQS-DG-NMCPProceedings@uscg.mil

Mail: Commandant (CG-DCO-84)
ATTN: Editor, *Proceedings* Magazine
U.S. Coast Guard Stop 7318
2703 Martin Luther King Jr. Ave. S.E.
Washington, DC 20593-7318

Web: www.uscg.mil/proceedings

Phone: (202) 372-2316

Subscription Requests

Proceedings is free.

Subscriptions
www.uscg.mil/proceedings



Maritime Governance

Designed with security in mind.

by Ms. DANIELLE BIVENS
Project Analyst
Java Production Incorporated

Our nation's increasing dependence on information and networked systems creates vulnerabilities that can threaten America's security. Recognizing this, the president signed Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, and Executive Order 13636, Improving Critical Infrastructure Cybersecurity,¹ and the Department of Homeland Security developed the National Plan to Achieve Maritime Domain Awareness.²

These policies foster information sharing and collaboration among federal and industry partners. Such collaboration is vital to identify potential cybersecurity incidents that could gravely damage critical infrastructure and significantly affect public health and safety, economic strength, or national security.

Consistent with these presidential policies, the National Plan to Achieve Maritime Domain Awareness provides the

maritime community with a common understanding of the magnitude of maritime security and the importance of enhancing maritime domain awareness.

Presidential Policy Directive 21

Already varied and complex in nature, the nation's critical infrastructure comprises distributed networks, wide-ranging organizational structures and operating models, and interdependent functions and systems in physical space and cyberspace. This complex infrastructure necessitates various levels of authorities and shared responsibilities in the public and private sector to attain a resilient critical infrastructure.

Presidential Policy Directive 21 guides efforts to secure, strengthen, and maintain the nation's critical infrastructure and directs critical infrastructure owners and operators to work together and share responsibility. This collaborative

approach seeks to reduce vulnerabilities, minimize consequences, disrupt threats, and improve response and recovery time for the maritime critical infrastructure.

Executive Order 13636

Repeated cyber attacks have endangered U.S. national and economic security. Executive Order 13636 directs the executive branch to:

- develop a technology-neutral voluntary cybersecurity framework;
- promote and incentivize cybersecurity practices;



Flag: Glen Jones/iStock/Thinkstock; Binary code: loops7/iStock/Thinkstock

- increase the volume, timeliness, and quality of cyber threat information sharing;
- incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure;
- explore existing regulations to promote cybersecurity.

Information sharing between the federal and private sector is key, so that these entities can better protect themselves from cyber threats. This is especially true for the U.S. Coast Guard, as it has always shared as much information as possible with industry and will continue to do so.

National Plan to Achieve Maritime Domain Awareness

The National Plan to Achieve Maritime Domain Awareness (MDA plan) provides timely, accurate, and informed decision making to anticipate potential threats and take effective and necessary action to mitigate those threats.

The MDA plan will help achieve maritime domain awareness by unifying the U.S. government and supporting international efforts with allies and partners around the world. To achieve this, the plan promotes sustaining favorable conditions for global maritime security and guides capabilities that efficiently share maritime information, including intelligence, law enforcement information, and all-source data from the public and private sectors.

MDA plan goals include:

- enhancing maritime domain transparency to detect, deter, and disrupt threats, as early as possible;
- enabling accurate, dynamic, and confident decisions and responses to the full spectrum of maritime threats and challenges through information sharing;
- facilitating partnerships to promote maritime domain information sharing, safeguarding, capacity building, and integration;
- preserving our nation's rights, freedoms of navigation and overflight, and uses of the sea and airspace recognized under international law, while promoting lawful, continuous, and efficient commerce flow.



Tashatvango/Stock/Thinkstock

Achieving these goals will make maritime domain awareness a critical national maritime security enabler, allowing leaders at all levels to make effective decisions that mitigate threats and challenges early, to ensure the prosperity of the United States, its allies, and its partners.

Looking ahead

While these cybersecurity policies will guide efforts to strengthen critical infrastructure security and resilience against evolving threats and hazards, this will not be an easy task.

The Coast Guard must employ an approach that includes information sharing between the public and private sector, so that all are able to coordinate to prevent, respond to, and mitigate cyber attacks.

About the author:

Ms. Danielle Bivens is a junior project manager with an M.S. in cybersecurity policy from University of Maryland University College. Her professional experience is in project management and she provides support to the U.S. Coast Guard Cyber Command.

Endnotes:

- ¹ United States. DHS. *Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience*. Washington, DC: Department of Homeland Security, March 2013.
- ² DHS. *National Plan to Achieve Maritime Domain Awareness*. Homeland Security. N.p., n.d.

The Coast Guard and Cybersecurity

A legal framework for prevention and response.

by LCDR BRANDY PARKER
Legal Counsel

U.S. Coast Guard Assistant Commandant for Prevention Policy

MR. GLENN GRAY
Law Student
Georgetown University



aetb/iStock/Thinkstock

Hackers hijack a waterfront facility's industrial control system, resulting in oil discharge into a navigable waterway. An access control system at another facility is hacked, allowing unauthorized persons access to the facility.

A vessel's navigation system is compromised, resulting in a temporary loss of vessel control. An oil rig's programmable logic controller is taken over by a disgruntled former employee, who tilts the rig, causing it to shut down.

These hypothetical scenarios demonstrate how our marine transportation system (MTS) is vulnerable to cyber threats.

In the wake of 9/11, Congress passed the Maritime Transportation Security Act, which charged the U.S. Coast Guard with protecting the MTS from physical and human threats.

Today, not only has the U.S. Coast Guard risen to this challenge, we have a variety of legal tools at our disposal to ensure the MTS is protected from cybersecurity threats that could lead to a transportation security incident.

Responsibilities of Sector-Specific Agencies

Cybersecurity is a national priority, and the responsibility to carry out this priority falls upon various sector-specific agencies (SSAs) throughout the executive branch.

In 2013, the Department of Homeland Security issued the National Infrastructure Protection Plan, pursuant to Presidential Policy Directive-21 (PPD-21),¹ which describes how various sector-specific agencies carry out cybersecurity responsibilities across the nation's critical infrastructure. The U.S. Coast Guard is the sector-specific agency² for the maritime transportation sector.

Sector-specific agencies provide institutional knowledge and specialized expertise. They lead, facilitate, or support the security and resilience programs and associated activities

continued on page 10

Legal Authority

Coast Guard personnel can draw upon various authorities to effectively prevent cyber attacks and accomplish cybersecurity framework goals.

The Maritime Transportation Security Act of 2002

Congress passed the Maritime Transportation Security Act (MTSA)¹ of 2002 in response to the large-scale, nationwide vulnerabilities that were exposed by the 9/11 attacks, with the goal to improve the physical and personnel security standards for ports, facilities, and vessels.²

MTSA focuses on prevention and response to transportation security incidents (TSIs), which are security incidents resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.³

U.S. facilities and vessels are required to conduct security assessments and implement security plans to address how they will deter a transportation security incident to the maximum extent practicable.⁴ The security plan must address how the facility or vessel will communicate with the federal government in the event of a security incident and include provisions for: maintaining physical, passenger, cargo, and personnel security; controlling access to security areas of the vessel or facility; and maintaining communications within the facility or vessel and with first responders.⁵

The Coast Guard implemented the Maritime Transportation Security Act through regulations in 33 CFR Subchapter H—Maritime Security.⁶ Cybersecurity is not specifically mentioned in MTSA or its regulations; however, many of the terms and requirements in MTSA and its regulations do encompass cybersecurity issues and cyber events. The reporting requirements in 33 CFR§101.305 illustrate this. Facility and vessel personnel are required to report suspicious activities, breaches of security, and TSIs immediately to the Coast Guard. Suspicious activities are described as those activities that may result in a transportation security incident,⁷ and a breach of security is an incident that, although it has not resulted in a TSI, security measures have been circumvented, eluded, or violated.⁸

The same holds true for vessel security assessments, which must evaluate many potential vulnerabilities, including the actual or potential vessel access points, the overall threat assessments for areas in which the vessel operates, security and safety equipment, communications systems, surveillance systems, and access control systems.⁹

This also applies to outer continental shelf facilities, which have proven to be vulnerable to cyber attack, due in part to their increased automation, which often includes wireless network access between shore operations and the facility.¹⁰

Although the Maritime Transportation Security Act does not prescribe specific measures that vessel and facility operators must take to protect cyber networks from attack, it does require that vessel and facility operators undertake the necessary measures to prevent transportation security incidents.

Many other parts of MTSA regulations address areas that are increasingly dependent on computer technology and are potentially vulnerable to cyber attack. For example, the Maritime Transportation Security Act requires vessel and facility operators to implement security measures for cargo handling that will deter tampering, prevent cargo not meant for carriage from being accepted and loaded, and identify cargo that is approved for loading on vessels.¹¹ In 2011, two major container terminals in Belgium were infiltrated by hackers who manipulated data about cargo containers to ship large quantities of drugs.¹² In that case, the hackers physically intruded the facilities and installed keystroke loggers onto terminal operating systems using USB drives.¹³

In the future, it is not difficult to imagine a scenario where this level of intrusion is achieved without ever physically encountering the computer terminals being hacked.¹⁴ Therefore, it is imperative that vessel and facility operators consider the cyber vulnerabilities of these systems.

Magnuson Act

First passed by Congress in 1950, the Magnuson Act authorizes the president to “safeguard against the destruction, loss, or injury from sabotage or other subversive acts,” and from accidents to “vessels, harbors, ports, and waterfront facilities.”¹⁵

As directed by President Johnson’s EO 11249, the regulations of the Magnuson Act were amended in 1965 to allow the captain of the port (COTP) to control or limit any “person, article, or thing” from gaining access to any vessel or maritime facility if such person, article, or thing is considered to be a danger to the safety and security of the involved vessel or waterfront facility.¹⁶

The Magnuson Act also allows the COTP to establish a security zone around any affected or potentially endangered vessel or waterfront facility when such a threat exists, and prohibits any person or object from entering a security zone without captain of the port permission.¹⁷ Further, the Commandant of the Coast Guard has the ability under the Magnuson Act to prescribe safety and security measures for vessels in port and waterfront facilities as he or she finds to be necessary to maintain vessel or facility security and safety.¹⁸

Under these provisions, a cyber attack or intrusion would certainly qualify as a potential danger and threat to a vessel or waterfront facility. An individual conducting a cyber attack against a facility by introducing a virus into a vessel’s control

continued on page 10





Among other protective measures, both the Magnuson Act and PWSA allow establishing security zones around at-risk vessels. U.S. Coast Guard photo by Petty Officer Kelly Newlin.

system would be the type of scenario where the captain of the port could use this authority to limit the individual or thing (virus) from gaining access to the targeted vessel or facility.

By using this authority to establish a safety or security zone around the vessel or waterfront facility, the COTP could block any future threats—whether from individuals or things—against the affected vessel or waterfront facility and other entities at risk. Furthermore, if the continuance or reoccurrence of a cyber attack warrants increased safety measures, the Commandant of the Coast Guard may prescribe such measures as he or she sees fit.

Ports and Waterways Safety Act of 1972

Congress passed the Ports and Waterways Safety Act of 1972 (PWSA) to protect ports, waterways, maritime facilities, and vessels from incidents involving negligence or sabotage. In 1986, under the International Maritime Port and Security Act,¹⁹ Congress amended the PWSA to allow the secretary of whichever agency the Coast Guard is operating under to “take actions ... to prevent or respond to an act of terrorism against an individual, vessel, or public or commercial structure that is subject to the jurisdiction of the United States;

and located within or adjacent to the marine environment; or a vessel of the United States or an individual on board that vessel.”²⁰

Such actions include inspections, port and harbor patrols, establishing security and safety zones, developing contingency plans and procedures, among others.²¹ In reference to the definition of “marine environment,” as stated in 33 U.S.C. 1226(a), such an area includes the waters of the U.S. exclusive economic zone and those above the outer continental shelf.²²

Currently there is not an official definition of terrorism codified in domestic or international law, but it is not difficult to think of a cyber attack against an individual, vessel, or public or commercial structure that would also be considered a terrorist act and thus trigger Coast Guard authority under the PWSA.

Endnotes:

- ¹ Maritime Transportation Security Act. 46 U.S.C. §§701 et. seq. (2002) [hereinafter MTSA].
- ² See MTSA at §70101 note.
- ³ See MTSA §70101(6).
- ⁴ See MTSA §§70102(b), 70103(c).
- ⁵ See MTSA, §§701013(c)(3)(B)-(C).
- ⁶ See 33 C.F.R. Parts 101, 103-06 (2014).
- ⁷ See 33 C.F.R. §101.305(a).
- ⁸ See 33 C.F.R. §101.105.
- ⁹ See 33 C.F.R. §104.305.
- ¹⁰ See Grant, note 10. See also, Indictment, *United States v Azar*, (C.D. Cal Mar. 17, 2009) (No. 09-00240). For OCS security assessment requirements, see 33 C.F.R. §106.305.
- ¹¹ See 33 C.F.R. §104.275(a) for vessels 33 C.F.R. §105.265 (a) for facilities.
- ¹² See Megan Gates, *Hackers Turn to Cargo Crime*, Security Management, at 12-13.
- ¹³ See Id.
- ¹⁴ Id. at 12 (“Container data logs have moved online and companies use electronic files, allowing criminals to hack into the system and change the data to make the shipment appear normal.”).
- ¹⁵ 50 U.S.C. §191(b) (2014).
- ¹⁶ 33 C.F.R. §6.04-5 (2014).
- ¹⁷ See 33 C.F.R. §6.04-6.
- ¹⁸ See 33 C.F.R. §6.14-1.
- ¹⁹ Pub L. No. 99-399 (Aug. 27, 1986).
- ²⁰ PWSA, 33 U.S.C. §1226(a)(1)-(2).
- ²¹ Id. (b)(1).
- ²² 33 U.S.C. §1222(1).

of their designated critical infrastructure sectors in the all-hazards environment.³ Moreover, securing the nation’s critical infrastructure cannot be adequately addressed by focusing on physical and personnel security alone. Therefore, cybersecurity is identified and emphasized as one of the three elements of critical infrastructure risk management, along with physical and human factors.⁴

Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity,⁵ focuses on critical infrastructure cybersecurity. In EO 13636, President Obama declared:

“[i]t is the policy of the United States to enhance the security and resilience of the nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency,

innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”⁶

The primary thrust of EO 13636 is the National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity and its push for the nation’s critical infrastructure owners and operators to adopt it.

The responsibility for encouraging adopting the cybersecurity framework falls largely on the SSAs. In addition, SSAs are directed to review their respective agency authorities for cybersecurity and cybersecurity framework goals.

Moving Forward

The marine transportation system is vulnerable to cyber threats, but the Coast Guard has the authority to respond to these threats.

The Maritime Transportation Security Act’s assessment and planning requirements should encompass cybersecurity vulnerabilities, as well as physical security and personnel security vulnerabilities. MTSA also requires the reporting of cybersecurity events to the Coast Guard when those events meet the definition of a suspicious activity, breach of security, or transportation security incident.

Once reported, the captain of the port can draw upon his or her authorities under the Magnuson Act and Ports and Waterways Safety Act to institute safety and security zones to limit access to the port and its facilities and to control vessel movement.

Using one or a combination of these authorities, the Coast Guard has a robust regulatory toolkit to help combat cybersecurity threats against the marine transportation system.

About the authors:

LCDR Brandy Parker is a U.S. Coast Guard attorney assigned to the Assistant Commandant for Prevention Policy. She provides legal and policy advice on matters of port security and prevention policy.

Mr. Glenn Gray is an intern for the U.S. Coast Guard with the Prevention Law Division in the Office of Maritime and International Law. He is also a law student at Georgetown University.



Maintaining compliance with MTSA’s provisions regarding facility and vessel access control is imperative to prevent cyber attacks. U.S. Coast Guard photo by Petty Officer Bobby Nash.

Endnotes:

- ¹ See Department of Homeland Security National Infrastructure Protection Plan [hereinafter NIPP]. The NIPP was created to guide the national effort to manage risks to the Nation’s critical infrastructure. The NIPP organizes the nation’s critical infrastructure into 16 sectors and designates sector-specific agencies (SSA) for each sector. Within the sectors, there may be subsectors that also have a SSA designated. See NIPP at 10. Each sector also has developed a plan for that sector that is an annex to the NIPP. See NIPP at 3, 9. The 2013 NIPP aligns with Exec. Order No.13636: Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739 (Feb. 19, 2013) and adds cyber elements into the physical and human elements of critical infrastructure in managing risk.
- ² SSAs are “responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.”
- ³ Presidential Policy Directive-21 (Feb. 12, 2013).
- ⁴ See NIPP at 15.
- ⁵ 78 Fed. Reg. 11,739 (Feb. 19, 2013).
- ⁶ Id.

C-Cubed

Increasing cyber resilience, awareness, and managing risk.

by MR. THAD ODDERSTOL
Director, Industry Engagement and Resilience
U.S. Department of Homeland Security

As U.S. ports are more reliant on technology, they must increasingly rely on the security of that technology. Insufficient cybersecurity leaves ports vulnerable to those who would disrupt the just-in-time delivery system that sustains U.S. commerce flow, which could also send a shockwave through the global economy.

However, cybersecurity experts are not just concerned about ports. Vessels are now equipped with integrated bridge systems, automation systems, and other increasingly complex technologies that are critical to maritime operations. Companies are also innovating and investing in high-seas

technologies to improve operational efficiency, including plans to develop an unmanned drone cargo ship.¹

So the marine industry must pay greater attention to the resultant threats and vulnerabilities through risk-based initiatives and stakeholder collaboration. Additionally, cybersecurity protection depends on many cyber systems (including computer networks) to connect ships, containers, and rigs.

In a competitive global landscape, maritime facilities must also protect sensitive business information and proprietary data. These efforts are critical not only to the maritime industry, but also to the industry's stakeholders in the U.S. Department of Homeland Security (DHS) and Department of Defense.

Improving Cybersecurity

To guide these efforts, President Obama signed an executive order and policy directive that focus on a "whole-of-community" approach to cyber resilience, where government and industry across the nation work together to make cybersecurity a priority.² The National Institute of Standards and Technology also developed the Framework for Improving Critical Infrastructure Cybersecurity, which consists of standards, guidelines, and best practices to promote critical infrastructure protection through cyber risk management.³

In support of these policies, DHS launched the Critical Infrastructure Cyber Community (C³ or "C-cubed") Voluntary Program, which is an innovative public/private partnership that aligns critical infrastructure owners and operators with resources to help them use the cybersecurity framework and manage their cyber risks.



Ship control board: Evgeny Sergeev/iStock/Thinkstock; Binary code: flik47/iStock/Thinkstock

The Three Cs

There are three key activities the program is supporting, which we emphasize as the **Three C's**:



Graphic courtesy of the Department of Homeland Security.

► **Converging:** C³ is converging critical infrastructure community resources to support cybersecurity risk management and resilience through the cybersecurity framework. DHS created a website at www.us-cert.gov/ccubedvp, linking its resources to support cybersecurity for public and private sector partners.

► **Connecting:** The program connects critical infrastructure stakeholders to the national resilience effort through advocacy, engagement, and awareness. This activity focuses on driving greater stakeholder participation, as well as re-engaging those who have been involved, to ensure all have access to available resources.

► **Coordinating:** The Critical Infrastructure Cyber Community Voluntary Program coordinates critical infrastructure efforts to maximize cybersecurity resilience, focusing on socializing cross-sector efforts, approaches, and lessons learned.

C-Cubed

The C³ program is open to any organization that is interested in using resources and engaging with DHS to develop guidance on how to implement the cybersecurity framework. Individuals may also opt-in as C³ community members and will receive free framework-related information and communication from the program via email.

The C³ Voluntary Program provides tools, services, best practices, and templates to:

- support industry to increase cyber resilience,
- promote cybersecurity framework awareness,
- encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management.

Online Resources



The Critical Infrastructure Cyber Community Voluntary Program features more than 30 DHS programs and tools, including a comprehensive program overview, downloadable tools, and outreach materials, all available online at www.dhs.gov/ccubedvp and www.us-cert.gov/ccubedvp.

Outreach

For example, companies and organizations may download an outreach and messaging kit that includes informational materials for easy printing and/or electronic distribution to help educate stakeholders regarding C³ and a slick sheet for chief executive officers and other leaders regarding cyber risk management.

Cyber Resilience Review

The DHS Cyber Resilience Review (CRR) is a voluntary, non-technical assessment that evaluates an organization's operational resilience and cybersecurity practices.

The CRR assesses enterprise programs and practices across a range of 10 domains, including risk management, incident management, and service continuity. It maps to the Framework for Improving Critical Infrastructure Cybersecurity, and allows users to conduct a self-assessment or access an on-site assessment that DHS cybersecurity professionals facilitate.

To learn more about the CRR or to download tools, visit www.us-cert.gov/ccubedvp.

Additionally, the program will engage with sector-specific agencies and organizations to develop guidance on how to implement the Framework for Improving Critical Infrastructure Cybersecurity, and then broaden the program's reach to all critical infrastructure and businesses of all sizes that are interested in using it.

The critical infrastructure cyber community will share resources and lessons learned and build a sustained community of interest around cyber risk, via C³. As more people become interested and want to reduce cyber risk to their organizations, this community will include a broader range of stakeholders. The vision is to offer a place for industry, state and local governments, and many other organizations to convene and discuss evolving cyber risk management needs and forge solutions.

The Maritime Industry

Of course, the maritime industry must be part of this effort to protect the economy and national security, and it must continue to provide innovative risk reduction and mitigation activities, as well as comprehensive maritime security and communication strategies. These strategies will be most effective if developed through collaboration with stakeholder partners and in accordance with applicable policies, procedures, laws, and directives.

While the C³ Voluntary Program was recently launched as a new program within the DHS Office of Cybersecurity and Communications, it is really an extension and refocusing of the department's long experience in working with industries across the country to transform their outlook on cybersecurity. The program reinforces DHS's larger risk-reduction mission and emphasizes the importance of an all-hazards enterprise risk management approach.

DHS invites maritime facilities and organizations to join the program and take advantage of its technical assistance, tools, and resources to ensure a more resilient critical infrastructure for a more resilient nation. In time, we hope the program will serve as a blueprint to sustain this interest in cybersecurity across the country.

About the author:

Mr. Thad Odderstol is the program director for the Industry Engagement and Resilience branch within the Department of Homeland Security's Office of Cybersecurity and Communications. The Industry Engagement and Resilience branch serves as the sector-specific agency to the information technology and communications sectors and provides guidance and expertise to the cross-sector critical infrastructure security and resilience community to address National Infrastructure Protection Plan cybersecurity requirements.

Endnotes:

- ¹ See www.bloomberg.com/news/2014-02-25/rolls-royce-drone-ships-challenge-375-billion-industry-freight.html.
- ² Executive Order 13636 *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive-21 *Critical Infrastructure Security and Resilience*.
- ³ Available at www.nist.gov/cyberframework.

For more information:

To join the C³ Voluntary Program or learn more about upcoming events, please visit
www.dhs.gov/ccubedvp
or **www.us-cert.gov/ccubedvp**
or email the program at **CcubedVP@hq.dhs.gov**

Reducing Cyber Risk

Marine transportation system cybersecurity standards, liability protection, and cyber insurance.

by MR. DAVID DICKMAN
Environmental Group and Maritime Group
Venable LLP

MR. DISMAS N. LOCARIA
Government Contracts Group
Venable LLP

MR. JASON WOOL
Energy Group
Venable LLP

Within our nation's marine transportation system (MTS), computers, information networks, and telecommunications systems support fundamental port and maritime operations. While this technology provides great benefits, it also introduces vulnerabilities.

In several recent incidents, bad actors exploited cyber weaknesses within MTS elements with significant repercussions. Some examples include:

- Somali pirates have exploited online navigational data to choose which vessel to target for hijack;
- hackers incapacitated a floating oil rig by tilting it and forcing it to shut down;
- malware caused another drilling rig to shut down for 19 days, after bringing systems to a standstill;
- hackers infiltrated computers connected to the Port of Antwerp, located specific containers, made off with smuggled drugs, and deleted the records.¹

Help is Here

Fortunately, MTS component owners and operators can take action to reduce cyber risk. The National Institute of Standards and Technology recently released the Framework for Improving Critical Infrastructure Cybersecurity, which allows users to leverage existing standards and guidelines² to tailor the framework to their specific needs and systems. For instance, MTS owners and operators using industrial control systems (ICS) will be able to choose guidance specific to those types of devices, such as NIST's SP800-82.

Given that the cybersecurity framework was specifically developed for owners and operators of critical infrastructure, each MTS sector member—including those who currently

follow established cybersecurity standards—should, at a minimum, access the framework to perform an internal assessment of its cybersecurity program.

Such an assessment is particularly relevant and, frankly, necessary, if owners or operators of ports, terminals, or other MTS segments have previously suffered a cyber attack or unexplained ICS failures. The Coast Guard considers such attacks or failures for vessels and facilities regulated under the Maritime Transportation Security Act to be reportable incidents under 33 C.F.R. 101.305 if such systems have connections to the MTS.³

Reducing Potential Liability

Despite the benefits of adopting the framework, MTS segment owners and operators should be aware that this alone is unlikely to completely limit potential liability following a cybersecurity incident. Two options that ports, facilities, vessels, and other MTS segment members should consider



The electric industry is subject to mandatory cybersecurity standards.



Anek_s/iStock/Thinkstock

It is important that ports conduct cyber vulnerability assessments.

to further reduce liability risk for cyber-related incidents are protection under the SAFETY Act and cybersecurity insurance.

The SAFETY Act

The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act⁴ allows businesses that sell anti-terrorism products, services or technologies, or that develop and implement their own cyber or physical security technologies, to mitigate a significant portion of their cyber-related risk by capping or even eliminating third-party liability arising out of designated “acts of terrorism.”⁵

The SAFETY Act provides two levels of protection—designation and certification. The process requires initial registration with the Department of Homeland Security (DHS), an optional pre-application process that includes DHS pre-application evaluation and a full DHS application review. The process can be lengthy and information intensive. For this reason, it is helpful to obtain legal advice and assistance to understand the act’s nuanced benefits and requirements and to navigate the pre- and post-award processes. Designation and certification levels are valid for five years and are subject to renewal in five-year increments thereafter.

Technologies and security programs that satisfy the designation-level requirements receive risk management protections, including liability caps at the amount for which the entity is insured, exclusive jurisdiction in federal court, and bars against punitive damages and prejudgment interest. Technologies and security programs with the higher certification-level receive all the benefits of designation, with the added benefit of providing immunity from third-party liability arising from an act of terrorism.⁶

Also, SAFETY Act approval could arguably reduce potential cyber liabilities that do not arise out of an act of terrorism by demonstrating that the organization took reasonable measures to minimize or mitigate a reasonable threat through its cybersecurity program, which has been vetted and deemed effective under the SAFETY Act.⁷

Cybersecurity Insurance

Finally, cybersecurity insurance has evolved in recent years to cover many of the contingencies that may occur as a result of cybersecurity incidents. It may be purchased as a stand-alone product or, in some cases, as part of a comprehensive policy. Those who operate ports, marine terminals, and other critical infrastructure businesses should closely examine their comprehensive policies with counsel to determine whether they cover cybersecurity incidents and losses.

Notably, implementing the cybersecurity framework or other well-known cybersecurity standards can be leveraged to great effect in the insurance context. Underwriters will typically only extend coverage to entities that have demonstrably strong security practices, and the framework or other standards can serve as a useful benchmark.

Moreover, robust cybersecurity practices could also lead to lower premiums. Some insurance brokers and providers have reduced premiums if the covered technology has received SAFETY Act designation or certification.

Moving Forward

Adopting cybersecurity standards, acquiring cyber insurance, and obtaining protection under the SAFETY Act for cybersecurity technologies can significantly reduce business risks as well as overhead expenses for ports, terminals, vessels, and other MTS segments.

Not surprisingly, those who operate airports, sea ports, and other critical infrastructure components have obtained SAFETY Act coverage for their physical security measures. The same should be considered for technology used to protect cyber-related infrastructure, including in the MTS.

The unfortunate reality, however, is that many businesses, including ports, marine terminals, and other MTS segments, even if they currently have strong cybersecurity programs and technologies, are unaware of the SAFETY Act and its protections. As cyber risk and the potential for increased liability related to cybersecurity within the MTS grow, however, the SAFETY Act may become better known, and, more importantly, utilized.

About the authors:

Mr. David Dickman is a member of Venable's Environmental and Maritime Groups. He is a retired Coast Guard officer with significant practical and legal experience on maritime security matters and has represented and advised ports and other MTS segment clients on security issues under the Maritime Transportation Security Act and other security laws and regulations. Mr. Dickman is a co-author on maritime security for Benedict on Admiralty. He has been recognized in the 2013 and 2014 editions of Chambers USA, in the shipping category.

Mr. Dismas Locaria is a member of Venable's Government Contracts Group. He represents a number of clients in homeland security-related matters including drafting guidelines for information handling. He has assisted several clients in receiving SAFETY Act certification. Mr. Locaria has published on the topic of the SAFETY Act and is a co-author and contributor to Venable's Homeland Security Desk Book.

Mr. Jason Wool is a member Venable's Energy Group and an experienced cybersecurity attorney who advises clients on the North American Electric Reliability Corporation critical infrastructure protection reliability standards and other cybersecurity standards and regulations. He contributed to developing federal cybersecurity regulation and policy, including the cybersecurity framework. Mr. Wool advises independent systems operators and regional transmission operators on reliability compliance and variety of other issues.



oim26250/iStock/Thinkstock

Endnotes:

1. Wagstaff, J. *All at sea: global shipping fleet exposed to hacking threat*, Reuters (Apr. 23, 2014). Available at www.reuters.com/assets/print?aid=USBREA3M20820140423.
2. Examples are ISO 27001/2 standards relating to information security systems and NIST's SP800-53 standard relating to security and privacy controls for federal information systems.
3. See www.uscg.mil/announcements/alcoast/122-14_ALCOAST.txt.
4. Subtitle G, of Title VIII, Public Law 107-296 (codified at 6 U.S.C. 441-444), available at https://www.safetyact.gov/pages/homepages/SamsStaticPages.do?insideIframe=Y&contentType=application/pdf&path=sams\refdoc\Safety_Act_Legislation.pdf.
5. An "act of terrorism" is an act, determined by the Secretary of DHS, that (i) is unlawful; (ii) causes harm to a person, property, or entity, in the United States or to a U.S.-flag vessel (or vessel based principally in the U.S. on which U.S. income tax is paid and whose insurance coverage is subject to regulation in the U.S.), inside or outside the U.S.; and (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the U.S. 6 U.S. Code§444(2).
6. The SAFETY Act's benefits apply not only to sellers/suppliers of technologies and to businesses that develop and implement covered security programs, but also to their customers. In fact, end-users (regardless of whether the technology is designated or certified) receive third-party immunity arising from acts of terrorism for utilizing a SAFETY Act-approved technology.
7. The scope of the SAFETY Act may be expanded in the near future, as a bill was recently unanimously approved by the House Homeland Security Committee that would provide coverage against "qualifying cyber incidents" that may not otherwise meet the definition of an Act of Terrorism. Sec. 202, H.R. 3696, National Cybersecurity and Critical Infrastructure Protection Act of 2013.

Bibliography:

- Chemical makers' cyber, physical security program approved for SAFETY Act liability coverage*. Inside Cybersecurity, March 4, 2014.
- Commander Joseph Kramek (2013). *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*. Center for 21st Century Security and Intelligence at Brookings.
- Commander Ulysses Mullins (2014) *Cyber Security: The boundary without borders*. *Proceedings of the Marine Safety & Security Council*.
- Dismas L., and Andrew Bigart. *SAFETY Act: A Cybersecurity Win-Win for Government*. Industry, Law360, Apr. 24, 2014.
- Analysis of Cyber Security Aspects in the Maritime Sector*. European Network and Information Security Agency, Nov. 2011.
- National Cybersecurity and Critical Infrastructure Protection Act of 2013. H.R. 3696, Wagstaff, J. *All at sea: global shipping fleet exposed to hacking threat*. Reuters, Apr. 23, 2014. H.R. 4005, Coast Guard and Maritime Transportation Act of 2014.
- Kouwenhoven, N., Martin Borrett, and Milind Wakankar. *The implications and threats of cyber security for ports*. Port Technology International, February 2014.
- Cybersecurity Alert: NIST Releases Framework for Improving Critical Infrastructure Cybersecurity*. Venable LLP, February 2014.

Cyberspace — the Imminent Operational Domain

A construct to tackle the Coast Guard's tough challenges.

by CAPT JEFF RADGOWSKI
Commander
U.S. Coast Guard Cryptologic Group

CAPT KATHERINE TIONGSON
Chief
U.S. Coast Guard Intelligence Plans and Policy

To ensure our nation continues to benefit from its maritime domain, we must also facilitate cyberspace safety. So, what does that mean for the Coast Guard?

To begin, it is important to define key cyber-related terms and provide background to understand this critical fifth domain alongside the physical domains of air, land, sea, and outer space.

Cyberspace and Cyber Supremacy

The Department of Defense (DOD) defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”¹ As an operational domain, cyberspace encompasses the electromagnetic (EM) spectrum (including the entire range of wavelengths or frequencies of electromagnetic waves from gamma rays to radio waves and visible light) and manmade electronic systems created to operate across this domain.²

“Future conflicts will be won in a new arena—that of the electromagnetic spectrum and cyberspace. We must merge, then master those realms.”

—Chief of Naval Operations
Admiral Jonathan Greenert, USN

For the Coast Guard, cyberspace activity starts in our work areas, with our computer systems, Internet, and smartphones, and extends to the complex command, control, communications, computers, intelligence, surveillance, and reconnaissance systems on cutters, small boats, aviation platforms, and at command centers.

In essence, we have transitioned into a wireless world, where we manage virtually all information through computer-based command-and-control systems. As such, CG personnel have a more pervasive dependency upon cyberspace than at any time in our history. Ironically, the very integration we seek to stay connected and optimize operational capabilities also presents vulnerabilities and challenges.

Battles for cyber supremacy already have a major impact on both geo-political and economic fronts. Events in recent years, such as the massive denial of service attacks against Georgia and Estonia³ and the plethora of politically motivated attacks against businesses and entire industry sectors, show the impact of the denial of freedom of information and disruption of systems dependent upon the Internet or government sites. Meanwhile, the successes of companies such as Google and Facebook clearly depict the value of Internet and social media market dominance.

Likewise, the nation's critical maritime infrastructure—the port facilities, refineries, waterways, locks, and dams—that control, process, and expedite the maritime transportation flow of goods to and from the U.S. are also critically dependent upon the electromagnetic spectrum and cyberspace.

No longer does the maritime industry rely on mule carts and manual intervention to move ships and cargo through waterways, but instead maritime workers manage all aspects through the EM/cyber domain, from monitoring vessel traffic movement to opening and closing flood gates. It's all done via the network.

Recognizing the Coast Guard's responsibility to protect and defend its own networks, the need to leverage cyberspace to maximize mission execution, and to facilitate the safety, security, and resiliency of the maritime transportation system, we must develop cyberspace capability and capacity, leveraging with a whole-of-government approach wherever possible. To that end, Coast Guard cyber priorities must be focused on:

- defending Coast Guard networks,
- protecting maritime critical infrastructure and key resources,
- developing cyberspace capability and capacity to enable mission execution.

While each of these priorities is challenging in its own right, the U.S. Navy's construct (know the environment, be agile, change our paradigm, the future is now) presents us with a relevant lens through which to consider when addressing the Coast Guard's own priorities.

Defending Coast Guard Networks

Know the Environment

To defend our own networks we must recognize the nature of the cyber environment and build better tools to sense the EM/cyber realm.

For example, sharing sensor information relevant to geolocations for a search and rescue case clearly enables Coast Guard missions. At the same time, spear phishing (personally targeted cyber attacks) and similar scams have proven to be powerful threats and weapons against our systems, considering the criticality of the information environment and the potential harm to networks we depend upon.

"Just as the United States dominates the maritime domain, we must do the same in the information realm, which includes cyberspace and the electromagnetic spectrum..."

**—U.S. Navy Admiral Michael Rogers
NSA director**

As such, the network is no longer a neutral space, but must be viewed as an operational domain where CG cyber personnel combat persistent threats and attacks. CG Cyber Command is at the front line of this defense, but depends

on all information technology users to act in a responsible manner. This requires developing a culture of security in cyberspace.

Be Agile

High-tech radars and sensory tools currently employed on Coast Guard cutters and aviation assets are highly detectable and easy to classify. This is another example of how successful tools aid our missions, yet can become vulnerabilities. When working through the acquisitions process, we need to be mindful of the risks and vulnerabilities associated with new systems and capabilities we plan to bring into the Coast Guard inventory. This also requires developing an effective concept of operations and doctrine for those systems.

"Future wars will not be won simply by effectively using the EM spectrum and cyberspace: They will be won within the EM/cyber domain." —U.S. Navy Admiral Jonathan Greenert

Future weapons, sensors, and information technology systems will need to employ various techniques to remain secure, including shifting frequencies, using shorter burst transmission, and employing small directional beams. Because, if we don't defend Coast Guard networks, we can't assure appropriate command and control.

Change our Paradigm

While the Coast Guard may not be considered a traditional "war-fighting" service, if we have learned anything from the last decade of cyber crime, terrorist activity, intrusions, and other nefarious activity, it is that we are all vulnerable.

We should not fool ourselves into thinking that our "noble" missions exempt or shield us from tremendously damaging exploitations and actions. A disgruntled person, criminal organizations, a hostile nation, or the 15-year-old who wants to make a statement will each have their own justifications for breaching Coast Guard systems and causing harm.

Coast Guard networks and systems hold the keys to its most protected and integral possessions as a service, including operational plans, strategy, or personally identifiable information. These may be the domains where any adversary can most readily and effectively strike with the greatest consequences. It's time to start thinking in these terms and developing a culture that protects and defends our networks. This effort should also include establishing more stringent criteria for those allowed special access, including system administrators, than we have authorized in the past.

“The relevance of information dominance has never been greater, particularly as our adversaries design new ways to exploit our networks and inhibit our mastery of the electromagnetic spectrum.” —U.S. Navy Vice Admiral Kendall Card

The Future is Now

Much of our efforts to promote security must be focused inward. The Coast Guard’s operational commanders should be concerned about the expanding number of critical ship-board and airborne systems (including combat, communications, engineering, positioning, navigation, and timing systems) that are networked, interdependent, and vulnerable to cyber attack.

We must develop a more holistic view of what constitutes the “network,” and commanders must understand that the Coast Guard is not outside the splash zone of the potentially crippling effects of attacks targeted at critical systems.

Protecting Maritime Critical Infrastructure and Key Resources

Know the Environment

The Global Positioning System jammer (a device that blocks, jams, or interferes with communications) constitutes a significant threat to our maritime transportation industry.⁴ The vast majority of U.S. commerce passes through our ports and waterways, so the maritime industry is especially vulnerable to these devices and similar cyber threats. Meanwhile, port facilities rely on networked computer control systems that span across domains.

The Coast Guard, in conjunction with its Department of Homeland Security (DHS) and port partners, must conduct maritime critical infrastructure and key resource (MCIKR) risk assessments that address cyber-related threats, vulnerabilities, and potential consequences. We must develop awareness of the full scope of port systems and how they are networked throughout ports and terminals.⁵ We must also ensure that regulations and maritime security plans identify or address potential cyber-related threats or vulnerabilities. Finally, we must leverage cyber capability to share cyber information among other government entities and our port partners to the same extent that we share other data to support mission success.

Be Agile

While the Coast Guard has already begun to aggressively address these issues, incorporating these into standard practices necessitates an “all hands on deck” effort, which

includes bringing public and private partners into the solution. Agility in this area should be easier for the Coast Guard than many other entities, given our ability to span military and law enforcement communities and our longstanding relationships developed with the maritime industry over the years. Using this to our advantage, we should leverage cybersecurity experts from government and industry in this effort.

Change our Paradigm

The paradigm of protecting maritime critical infrastructure is turned on its head with the cyber component; therefore addressing jammer threats and port cybersecurity vulnerabilities is only part of the solution. The Coast Guard can leverage various risk assessment tools to better assess cyber risks. MCIKR exercises and workshops will also point to currently unseen areas for improvement, so the Coast Guard can readily apply lessons learned to champion similar exercises for all stakeholders involved in protecting critical infrastructure. These exercises simulate and will pave the way to how we will execute cyberspace operations.

The Future is Now

Unfortunately, we no longer have any lag time to get these efforts underway. It’s no longer a question of “if” MCIKR cyberspace vulnerabilities will lead to cybersecurity incidents, but “when.” Given our national dependency on maritime critical infrastructure and key resources, the Coast Guard and its interagency and industry partners cannot afford to delay implementing proactive measures needed to address deficiencies.

Developing Cyberspace Capability and Capacity

Continuing to develop cyberspace capabilities will strengthen the Coast Guard’s ability to defend its networks and protect maritime critical infrastructure. Doing so will also enable the service to attain intelligence-based maritime information advantage and the ability to act on that intelligence in the cyberspace domain. Likewise, we must be proactive in identifying current and planned DOD and DHS initiatives that contribute to achieving the objectives.

Know the Environment

As the nation’s leading national maritime governing organization, the Coast Guard must continue to address current and future threats throughout all operational domains impacting the maritime environment. With cyber growth continuing at breakneck speed, achieving a complete common operating picture and improved maritime domain awareness has never had more relevance or presented a greater challenge.

The signal-to-noise ratio (the ratio of useful information to false or irrelevant data) is smaller than ever, and trying to figure out which of those signals is valuable gives a new meaning to “hiding in plain sight.”

Additionally, the cyber flash-to-bang time is far quicker than the kinetic version. When the Coast Guard cannot utilize its intelligence to conduct timely cyberspace operations, it risks more than just its networks—it jeopardizes its ability to execute missions. Therefore, our cyber-based intelligence must constantly monitor, identify, and neutralize these threats.

Be Agile

The Coast Guard must identify its most relevant threats and cue our operational response to address them. To accomplish this, we must deconflict the growing number of military and civilian EM/cyber systems. Additionally, we must continuously update our systems to ensure they are meeting our cyber needs. This effort requires a commitment to continued and increased cooperation and collaboration across the cyberspace community. Agility with respect to personnel requires a similar construct to build our cryptologic expertise in the Coast Guard—leverage training wherever possible and strategically place personnel within key nodes throughout DOD and the intelligence community to provide the maritime perspective other agencies may not have an understanding or appreciation for, while also building our knowledge and skills that will reap great benefit for the Coast Guard. We have started that effort integrating Coast Guard personnel within USCYBER Command and in key cyber-focused offices within the National Security Agency; however, we must remain vigilant to opportunities within the combatant commands, Navy elements, DHS, and elsewhere that may provide similar return on investment for the Coast Guard. This effort also requires alignment of cyberspace workforce policy, recruiting, training, and retention efforts with DOD, as feasibly possible.

“Those hostile to the United States incessantly exploit our networks, necessitating our constant vigilance and aggressive, intelligent action... .”

**—U.S. Navy Admiral Michael Rogers
NSA director**

Change our Paradigm

The Coast Guard has historically employed linear case building for intelligence-driven operations—layering elements of intelligence in relatively small pockets to tactically cue missions. In today’s world of pervasive cyber threats, this mode of operations is no longer feasible or tenable. Experience has taught us that we must share information over a broad,

diverse range of stakeholders in real time and allow many analysts to collaborate and correlate this disparate data for successful mission execution. Similarly, a critical criteria for future Coast Guard capabilities must be system interoperability and integration with our DOD partners, particularly the Navy, as well as key DHS components. Systems that interact can extend the footprint of one unit or asset alone, providing an extension of otherwise limited capabilities.

The Future is Now

While increasingly constrained budgets force the Coast Guard to make tough programmatic and fiscal choices, this does not obviate or postpone the need to make appropriate investments in cyberspace capabilities. Many initiatives are cross-governmental or come with resource contributions to gain equities (cloud-based, IC ITE, and object-based production, for example). We must take advantage of every possible opportunity to learn from others and leverage initiatives to make the most of the resources we do have.

Moving Ahead

It is clear that cyberspace is a critical operational domain to the Coast Guard. Like many U.S. government organizations have done, we too must take the appropriate actions in the domain to facilitate Coast Guard missions that are critical to the nation.

To accomplish this, we can learn from our Department of Defense and other partners to frame questions and drive the actions we can take today to ensure successful mission execution in the cyberspace operational domain.

About the authors:

CAPT Jeff Radgowski is the commander, U.S. Coast Guard Cryptologic Group. He has served in the Coast Guard for 24 years since graduating from the U.S. Coast Guard Academy. He is a professionally licensed mechanical engineer and holds an M.S. in ocean engineering, an MBA, an M.A. in international relations and homeland security, and an M.S. in strategic intelligence.

CAPT Katherine Tionson is the chief of Intelligence Plans and Policy at Coast Guard headquarters. She has served for 25 years since graduating from the Coast Guard Academy in 1989 as a government major and holds an M.S. in strategic intelligence.

Endnotes:

¹ CJCS Joint Pub 3-12.

See Deputy Secretary of Defense Memorandum, Subject: *The Definition of Cyberspace*, May 12, 2008.

² Air Force Cyber Command Strategic Vision, Feb. 2008.

³ http://ccdcoc.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf.

⁴ Intentional high-power jamming incidents in South Korea in 2010, 2011, 2012 cumulatively affected more than 300 cell towers, 1,000 planes, and 250 ships.

⁵ GAO Report on Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity, June 2014. Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate. GAO-14-459.

Shifting the Paradigm

The DHS Continuous Diagnostics and Mitigation Program.

by MR. ERIC GOLDSTEIN

*Policy Advisor, Federal Network Resilience
U.S. Department of Homeland Security*

MR. MARK KNEIDINGER

*Senior Advisor, Federal Network Resilience
U.S. Department of Homeland Security*



Alex Skopje/iStock/Thinkstock

Cyber threats present an increasing risk to the safety and security of Americans, jeopardizing our economic prosperity, national security, and way of life. To minimize the likelihood of damaging cyber attacks, the Department of Homeland Security (DHS) is implementing the Continuous Diagnostics and Mitigation (CDM) program to protect government networks.

For the first time, the federal government will know the state of its networks at any given time, identify and rank problems for priority resolution, and invest resources in fixing the most significant cybersecurity problems first.

Background: A Heightening Risk

Critical infrastructure systems—including electricity, transportation, water, and communications—are crucial to America's economy, security, and way of life. Additionally, government departments and agencies maintain personally identifiable information, national security information, and law enforcement information, and the government provides critical functions, from Social Security payments, to ship-to-shore communications, to air traffic control.

All of this infrastructure uses information and communication technology. Most Americans, too, use the Internet daily for myriad activities, which provides productivity, efficiency, and societal benefits.

However, adversaries can exploit our reliance on information and communication technology and the Internet and

cause highly damaging incidents that can cause significant economic harm and the potential for disrupted infrastructure and even loss of life. Bad actors are increasingly resourced and sophisticated and have adapted to operating in contested environments.¹ Such threat actors may be highly motivated nation-states or organized criminal groups, seeking specific information or attempting to achieve a particular functional objective through a cybersecurity vector. In many cases, the defenses arrayed against such malefactors may be insufficient in speed, depth, and timeliness.

The Defense

So the U.S. government must assemble resources to respond to this increasing risk. As funding so often follows priorities, the federal government spent an estimated \$13 billion on cybersecurity activities in fiscal year 2014.² The question

Continuous Diagnostics and Mitigation Phases

- **Protect end-point devices:** Scan and ensure devices are identified and properly configured.
- **Manage users and their permissions:** Make sure that users only have access to the information for which they are authorized.
- **Manage events:** Rapidly identify, respond to, and mitigate cybersecurity issues and threats.

remains, however, whether such investment and executive focus has resulted in measurably improved security for sensitive government data and essential services.

For example, the 2002 Federal Information Security Management Act (FISMA) facilitated National Institute of Standards and Technology standards and guidance that provide a basis for common cybersecurity risk management practices. However, many aspects of FISMA compliance and implementation were traditionally administered via manual security control testing. Given the agility of cybersecurity threats, manual control testing is often inadequate to protect government systems or provide a valid understanding of cybersecurity posture.

Further, under the current FISMA approach, federal agencies conduct thousands of assessments and write and issue reports. Sadly, this information is out of date the moment it is printed, as it provides only a snapshot versus real-time, dynamic problem identification. In large civilian agencies, this paperwork can account for as much as 65 percent of the overall IT security effort.

In this paradigm, attackers consistently outpace these moribund protection efforts. Therefore, the Office of Management and Budget codified the Continuous Diagnostics and Mitigation Program, requiring federal agencies to adopt an information security continuous monitoring program.

CDM Concepts and Principles

In brief, continuous diagnostics and mitigation provides federal civilian agencies with sensors to detect cybersecurity issues on an ongoing basis and services to ensure that these sensors are effectively installed, integrated, and operated. Specific cybersecurity issues are displayed on agency dashboards for corrective action, and a federal dashboard will provide summary information on each civilian agency, allowing comparisons of cybersecurity posture across the executive branch.

CDM begins when an organization installs continuous diagnostics sensors on its networks that scan for cybersecurity

The CDM Process or “How CDM Works”



The CDM Program enables government entities to expand their continuous diagnostic capabilities by increasing network sensor capacity, automating sensor collections, and prioritizing risk alerts. This approach lowers the operational risk of information security systems and .gov networks. Graphic courtesy of the Department of Homeland Security.

weaknesses, such as unauthorized hardware, unpatched vulnerabilities, or insecure configuration settings. Detailed results of these ongoing scans are sent to a dashboard that the responsible department or agency maintains, and summary results are sent to the DHS federal dashboard.

At the department/agency level, personnel prioritize specific cybersecurity weaknesses based upon impact and threat, and rank them for resolution. At the federal level, staff aggregate summary results to provide a single grade reflecting the overall cybersecurity posture.

Departments and agencies are responsible to mitigate cybersecurity weaknesses, based upon the prioritized list on the local dashboard. The prioritized weaknesses list is then updated on the local dashboard based upon mitigations and upon ongoing scanning. Department/agency grades will change, as the scored summary weaknesses decrease. Finally, CDM sensors are updated, as required.

Addressing a National Concern

Continuous diagnostics and mitigation is a strategic response to a national concern—the increasing vulnerability of sensitive information and essential services to motivated and highly competent adversaries. *Ad hoc* approaches

CDM Benefits

Speed: Continuous diagnostics and mitigation expands existing capabilities to automatically identify cybersecurity weaknesses in near real-time. This helps risk managers and system administrators understand network risks and allows a common operational picture of network health and integrity. Further, identifying cybersecurity weaknesses on an ongoing basis enables personnel to mitigate many of the worst problems before an adversary can exploit them.

Prioritize resources: Under existing cybersecurity approaches, it is tempting to target resources—whether personnel, technology, or other investments—toward fixing the most significant problems first. However, this constrains effective risk management. It is more feasible to allocate resources toward the problems that are most likely to result in a cybersecurity incident, or that would lead to significant impact.

Unity of effort: Through continuous diagnostics and mitigation, information security personnel can be focused on positive security outcomes based upon a common lexicon. By structuring performance around measurable outcome, as opposed to output or process, cybersecurity managers can justify resources and hold a clear sense of mission. Further, CDM provides cybersecurity staff with a “to-do list” of the most important weaknesses on a given network, ensuring that their activities are integrated around a common set of problems.

Valued metrics: CDM enables users to compare cross-agency performance by identifying and prioritizing cybersecurity risks based upon standard criteria and data (known as risk scoring). This allows agencies to understand how their particular cybersecurity posture compares to similar organizations and will improve oversight fidelity.

Strategic sourcing: A constrained budget environment challenges agencies in every branch and level of government in terms of increasing cybersecurity requirements. Fortunately, a CDM blanket purchase agreement provides significant cost savings on commercial products and services through bulk purchasing discounts. Further, CDM tool and service discounts are also available to state, local, tribal, and territorial governments.

to cybersecurity have proven inadequate, as have solutions based solely upon compliance rather than outcome. By moving the entire civilian federal government toward ongoing assessment and prioritized mitigation, CDM advances the state of cybersecurity to a pace commensurate with the threat.

However, continuous diagnostics and mitigation alone is not the entire solution. System users must be trained in and adhere to appropriate security practices. Oversight entities will need to hold departments and agencies accountable and federal acquisition capacity will need to nimbly incorporate innovative cybersecurity solutions.

It will require a whole-of-society approach to protect the nation from cybersecurity risk and ensure that the Internet remains a driver of our prosperity, values, and shared growth. CDM is one significant step in advancing the government toward assuring that our networked future is safe, secure, and resilient.

About the authors:

Mr. Eric Goldstein is a policy advisor in the Federal Network Resilience division of the DHS Office of Cybersecurity and Communications, where his portfolio includes training and governance for the Continuous Diagnostics and Mitigation Program. Previously, he served at the Homeland Security Studies and Analysis Institute (a federally funded research and development center supporting DHS), and held homeland security positions in state and local government.

Mr. Mark Kneidinger is senior advisor of the Federal Network Resilience division, within the Department of Homeland Security's Office of Cybersecurity and Communications. He leads outreach and engagement for the Continuous Diagnostic and Mitigation Program and manages a number of strategic initiatives. Prior to joining DHS, he held leadership and several senior positions, including as a chief information officer and as a deputy assistant secretary for the U.S. Agency for International Development.

Endnotes:

¹ For a broader overview of cybersecurity threats, see: Applegate, Steve and Angelos Stavrou. *Toward a Cyber Conflict Taxonomy*. 5th International Conference on Cyber Conflict. 2013.

² *Federal Information Technology FY 2014 Budget Priorities*. Available at www.whitehouse.gov.

Hacking 101

Using social engineering increases security attack effectiveness.

by MR. RON SCHNELL
*Adjunct Professor of Computer Security
Nova Southeastern University*



In 1982, I was 15 years old, attending a boarding school in Massachusetts. A good friend of mine was a well-known hacker who taught me how to use social engineering to gain access to protected systems, obtain secret information, and even cause people to perform actions that they should not have.

As hackers (or friends of hackers) do, I wanted to show my classmates how it was done. They gathered around the dorm payphone as I lifted the receiver and dialed “0” for operator. In those days, there were actually people at consoles helping you with phone calls, answering questions, or even interrupting a phone call in case of an emergency.

The call went something like this:

Operator: Operator, can I help you?

Ron: Yes, this is Bob from TSPS Engineering. I need to run a test on your station.

Operator: Um, okay sure.

Ron: I need you to type the following on your console: KP, two zero one, five, five, five, three, eight, four, nine.

Operator: Okay

Ron: Okay, now I need you to press ST and please go “No AMA” on that, alright?

Operator: Yes, sir.

A second later, I was connected to a number in New Jersey—for free. At the time, that call would have cost me several dollars, but I didn’t even put a dime into the phone.

acidgrey/iStock/Thinkstock

Why Did This Work?

So, why did the operator do what I asked? First, I knew the “lingo.” TSPS was shorthand for the operator’s position (Traffic Service Position System), so “TSPS Engineering” sounded legit. Pressing the “No AMA” key assured that the call would not be billed.

This knowledge allowed me to speak with confidence and to sound convincing that I was who I said I was, so the operator trusted me and did what I asked.

Using lingo helps create trust, because the person sees whoever uses the lingo as being one of them or understanding them, so is more likely to trust that person.

By nature, human beings want to be helpful. By default, when someone claiming to be of authority asks us to do something, we want it to be authentic. When we find any evidence at all that it is, we naturally cling to it and we feel relief.



Hlib Shabashnyi/iStock/Thinkstock

Social Engineering

Social engineering is an extremely successful attack vector in the private sector. Companies spend millions of dollars securing their technology infrastructure with firewalls, the strongest encryption possible, and passwords that are so complicated that they would be nearly impossible to crack.

But all of this means nothing if a clerical worker does the bidding of a stranger. My hacker friend once said to me, “Why try to hack through someone’s security when you can get someone to open the door?”

Sometimes, in high-security applications relating to government or extraordinarily high-valued assets, there are strict processes and procedures in place to deal with personnel authentication. But an expert social engineer knows how to cause a person to toss all training aside by employing two common techniques—urgency and fear.

Urgency and Fear

When a target receives a telephone call that is purported to be urgent, there is a natural desire to shortcut things. For example:

“Hello, this is Dr. Carter at New York Hospital. Mr. James has been in a horrible accident and we need access to some of his records immediately! Kim James is here with me now, and she says that those records are on his computer, but she doesn’t have the password. Can you please change it to something for us?”

Assuming Mr. James is the CEO of the company, this lowly worker on the phone faces the dilemma of following security protocol and potentially challenging the boss’s wife, or being a hero and saving the boss’s life. Another call might involve masquerading as a huge client, who is threatening to go to a competitor if he can’t get access to

his account immediately, and there are millions of dollars on the line. You can imagine that, in these scenarios, a low-level employee or call center worker does not want to be the person to cause irreversible damage to a company or organization.

Lingo

Successful attacks like the TSPS Engineering example show the value of lingo. Urgency and fear are effective, but when combined with lingo, attacks become that much more successful. I am fascinated with lingo, and my thirst for it never ends. Not because I perform social engineering exploits, but because people feel like they can be closer to you when you speak their language. I call myself a “lingoist,” which is a term I invented for someone who studies lingo.

When I am near specialists of any kind and they are using any sort of lingo, my ears perk up, and I take mental notes. Later, when I meet the same type of specialist, I throw in the same lingo and watch how it works. However, this can be dangerous.

For example, when a relative was in the hospital recently, I liberally used lingo in front of the nurses, asking about “sats” (oxygen saturation), certain heart rhythms, and even asking whether a chest tube happened to be a “32-French.” After several minutes of this chatter, the nurse eventually asked me whether she should give the patient 50mg or 100mg of a medication. She assumed that I was a doctor.

Social engineering:

“The practical application of sociological principles to particular social problems.”

—American Heritage dictionary

“Any act that influences a person to take an action that may or may not be in their best interest.”

—www.social-engineer.org

One would think (as she did) that someone would have to have gone to medical school or at least nursing school to know that lingo. In reality, I learned it all from the television show ER. Many television shows have producers or consultants who ensure that the lingo and technical aspects of the show are correct. Law

enforcement has been plagued by the “CSI effect” for years, because the show is so realistic.

There are many other sources of lingo, including overheard conversations, radio scanners, and vocational training. All of these methods (including television) have the advantage of being able to hear how words are pronounced. Although the Internet, books, certification tests, and training materials are a rich source of lingo, pronunciation is usually not a part of those materials. If a social engineer is attempting an attack and mispronounces some lingo, the attack will surely fail more quickly than if lingo had not been used at all.

Successful social engineers know this. I've witnessed people gain information or access, despite the highest level of security imaginable, using lingo and confidence. It is extraordinarily difficult for someone to overcome human nature and the desire to be helpful, the tendency to trust, and the fear of getting into trouble.

Process and Procedure

It is possible to maintain an organization or company that can defend against these sorts of attacks, but it requires ongoing training, and trainees must be made very aware of social engineering techniques. Additionally, this training must extend to the lowest-ranking person in the organization, even if that person has no access to sensitive data or capabilities.

Why should someone who doesn't even have access or capabilities be trained for this circumstance? It can be surprising how resourceful someone can be when they think there is an emergency, they fear failure, or believe they have a chance to be a hero. The target can even become an unknowing advocate for the attacker and extend the attack to superiors.





It may seem silly, but regularly performing surprise social engineering attacks on one's own organization is the best way to prepare personnel to deal with such attacks. Military organizations regularly perform drills regarding physical attack, or even cyber attacks. Social engineering attacks should be another sort of drill.

Process and procedure are already important parts of any military organization and most successful companies. But it is important that they account for situations of apparent duress, as well as nominal situations. There should be something in place for when a hysterical person calls with some emergency that would require a departure from the normal procedure to mitigate the situation.

This procedure might be to treat it exactly the same as any other request for information or action, even in "life or death" situations, or it could be a streamlined process, as long as the authentication portion doesn't short-circuit certainty.

Red Flags

There are certain red flags that can be apparent during a social engineering attack, including:

-  **Refusing to give contact information:** Oftentimes, the attacker will make up an excuse, or even feign a bad connection.
-  **Rushing:** If someone is in an inexplicable hurry to get to conclusion, it can indicate that the person is a bit too eager to finish the telephone call or exchange.
-  **Name-dropping:** A social engineering attacker is apt to drop names in addition to lingo, to put the target at ease.
-  **Intimidation:** A person with legitimate access would not (or should not) use intimidation to insist on authority, apart from proper procedure.

Staff or personnel should be trained to look for these red flags, in spite of lingo, when evaluating whether a request or command is authentic. They should also be trained to see lingo for what it is—shorthand that bad actors can use against you.

By having these processes in place, if there is an emergency, the person calling will be expecting nothing more and nothing less, and the person answering the telephone will not have the dilemma of having to improvise against standard procedure, as this is an expected eventuality.

About the author:

Mr. Ron Schnell is an adjunct professor of computer security at Nova Southeastern University in Ft. Lauderdale, Florida, and a principal at Berkeley Research group. He has been in the software industry for more than 30 years, having worked at Bell Laboratories, IBM, and Sun Microsystems. He began lecturing at NYU's Courant Institute of Mathematical Sciences in 1981, when he was 14 years old, and travels the world speaking to students, companies, and organizations.

Zero-Day Vulnerabilities

What to do when it's too late to prevent an attack.


by PROF. XIUWEN LIU
Florida State University

PROF. MIKE BURMESTER
Florida State University
and Director, Center for Security and Assurance in IT

MR. FRED WILDER, CAPTAIN USCG (RET.)
Maritime Technology and Port Security Consultant

MR. W. OWEN REDWOOD
Ph.D. student
Department of Computer Science
Florida State University

MR. JUDD BUTLER
Partner
Educational Development Group



Computers are designed to execute programs, which consist of instruction sequences. An instruction not only performs its operation, it also points to the next instruction. Instructions are written as zeroes and ones and are executed faithfully, regardless of mistakes or bugs.

A bug, however, can change the next instruction completely. Security vulnerabilities are essentially bugs that can be used to build exploits—sequences crafted to perform malicious actions.

Kheng ho Toh/Hemera/Thinkstock

A “zero-day” vulnerability is a previously unknown technological susceptibility or weakness—typically discovered after it has been exploited. So there are zero days between the time the vulnerability is discovered and the first attack. Put simply, hackers discover the vulnerability and exploit it, before developers can fix it.

For example, the Heartbleed vulnerability created the opportunity for hackers to steal passwords, keys, and other sensitive information.¹ This vulnerability existed for more than two years before detection and affected more than 600,000 secure websites, including government agencies, banks, and critical infrastructure. Because computers are ubiquitous in

ports and vulnerabilities always exist, protecting that infrastructure from cyber attacks is a pressing need.

Zero-Day Vulnerabilities, Exploits, and Attacks

For cyber criminals, unpatched vulnerabilities in software are free passes to attack any target using this software. Generally, there is little defense against a zero-day attack. Once it is used, however, it runs the risk of being discovered by the security community, thus most zero-days have limited lifespans. Nonetheless, zero-day attacks can cause widespread damage to critical infrastructure in one simultaneous attack across many targets, including seaports.

Nation-states, criminal organizations, terrorists, or other malicious actors could target seaports for smuggling, espionage, sabotage, or to cause great human and economic harm for political reasons. For example, ports often manage containers through a computerized logistics system. A hacker could disrupt the container routing and storage process, causing chaos and certainly delaying transport.

Another scenario involves a port's automated ship routing from the sea buoy to its assigned berth at the port. In this process, the shipping agent fills out a berthing request online, and the ship is assigned an arrival time and berth. This serves as a contract between the ship and port that facilitates expeditious cargo offloading and loading. If this online routing system were hacked, the port might receive hundreds of berthing requests each minute, triggering an override in the berth assignment system and bringing routing to a standstill.

Vulnerability Assessment, Penetration Testing

To mitigate these types of cyber attacks, computer analysts seek to identify vulnerabilities in the seaport's critical computer network infrastructure. For example, analysts will conduct a vulnerability assessment to identify, quantify, and prioritize security weaknesses. The assessment process involves reviewing system characteristics like assets, settings, specifications, code, and traffic.

Another method is to conduct penetration testing and attempt to attack the system as a hacker would—using discovered vulnerabilities to “break” the system. Analysts gauge the significance of such breaks by the impact on three security objectives:

- confidentiality,
- integrity,
- availability.

Confidentiality is the most important security goal. However, for most critical infrastructures, guaranteed availability is also essential to monitor and control sensors and equipment.²

The goal of each method (vulnerability assessment, penetration testing) is to find vulnerabilities hackers could exploit to gain unauthorized system access and fix them before hackers find them. The level of assessment rigor is determined by the associated risks, so it is typically combined with systematic risk analysis.

Prevention and Mitigation

Zero-day exploits have thus far only been used in targeted attacks, as will likely be the case in the future.³ For websites that are not an initial attack target, the best mitigation practice is to consult publicly disclosed vulnerability lists

in a timely manner, as once a vulnerability is disclosed, an invisible race between malicious hackers and security teams is on. All vulnerable components should be patched immediately; if patches are not available, security teams must analyze the exploits and explicitly block them.

Ideally, one would like to prevent zero-day exploits completely; however, this is easier said than done. Traditionally, antivirus software relies on signatures to identify malware, but zero-day exploits have no specific signatures prior to discovery. That means anti-virus and other signature-based security products cannot detect them.

However, malicious activities are intrinsically different from normal activities in terms of networking patterns, data packet patterns, and command usage. Analysts can use these characteristics to detect zero-day exploits via network pattern analysis.

In addition, exploits typically involve a number of stages to be successful; breaking any of the stages will stop the exploits. Therefore, it is essential that organizations take a holistic approach to carefully examine all aspects of its network infrastructure and network activities to minimize exposed surfaces.

There are three general approaches to prevent and mitigate zero-day exploits:

- **Network-centered approaches:** Zero-day vulnerability exploits require distinctive patterns that are very different from normal patterns in network packets. More general rules to detect suspicious packets could detect packets trying to exploit vulnerabilities. Unfortunately, due to the unknown nature of zero-day exploits, these approaches have a higher chance of rejecting valid requests (more false negatives) than methods detecting known threats via unique signatures.
- **Host-centered approaches:** Monitoring activities on individual servers and desktops can also identify zero-day attacks. Via application whitelisting, system

Black, White, Gray

In a penetration test, the testers receive information about the infrastructure. That disclosed information can range from no information about the system structure, known as black-box testing, to full disclosure (network diagrams, source code, IP addresses, and such), known as white-box testing. Any disclosure between the two extremes is gray-box testing.

US-CERT

Users can report exploits that use malware (such as computer worms and viruses) to computer security incidence response teams such as the United States Computer Emergency Readiness Team (US-CERT).

This agency publishes current activity reports and regularly updates summaries of the most frequent, high-impact security incidents to mitigate the impact of such exploits through timely information aggregation and reporting.

In February 2013, US-CERT launched the Critical Infrastructure Cyber Community Voluntary Program to help improve critical infrastructure cybersecurity system resiliency.

security teams allow only approved programs to run, while blocking all other programs.⁴

- **Security policies:** Security policies must be enforced to limit an organization's exposure to zero-day vulnerabilities and associated exploits. For example, some organizations do not allow applications and programs to be loaded on their computer system without first sanitizing them.

Best Security Practice Guidelines for Seaports

Cybersecurity and physical security are increasingly interconnected. Consequently, close collaboration among cyber analysts and physical security professionals is essential for maritime transportation and other critical infrastructure sectors. Fortunately, the most effective solutions do not involve new approaches or strategies, but instead focus on rigorously applying known methodologies.

Security-Oriented Device and Application Configuration

The goal is to configure devices and applications to bypass functionalities that have security risks as well as remove unneeded programs to reduce system vulnerability. Complexity is security's worst enemy—the smaller its attack surface is, the more secure a website becomes.

Keep operating systems and firmware up to date: System security personnel should regularly update computer and firmware operating systems and apply all bug and security fixes immediately. No application can be secure if its operating system is vulnerable.

Ensure that network devices and applications do not expose system information: Configure Ethernet routers, switches, and applications to give only the information required to support active applications, end users, and customers. Be sure no information about system configurations can be derived from application and system names.

Install only required and approved applications: Install only required applications and regularly approve and maintain them. Unused programs put extra maintenance burdens on the cybersecurity team and could create additional security threats.

Partition the network: Partition the network into multiple segments to host users and applications with different levels of security requirements. This is an effective way to contain damage, in case of a network intrusion.

Enforce a BYOD (bring your own device) policy: Mobile vulnerabilities have increased dramatically, so consider limiting smartphones and personal devices to the open segment of the network. Sanitize and properly configure all personal devices. Many critical infrastructure sites completely ban smartphones, personal devices, and removable media devices for well-founded security reasons.

Fix default and weak passwords: In many cases, passwords are the only way to distinguish a valid user from an attacker. Weak passwords can be cracked and therefore broken, giving an attacker easy access to the system. Similarly, change default and weak passwords on devices and applications. Require strong credentials to reset passwords. Use two-factor authentication for important applications.⁵

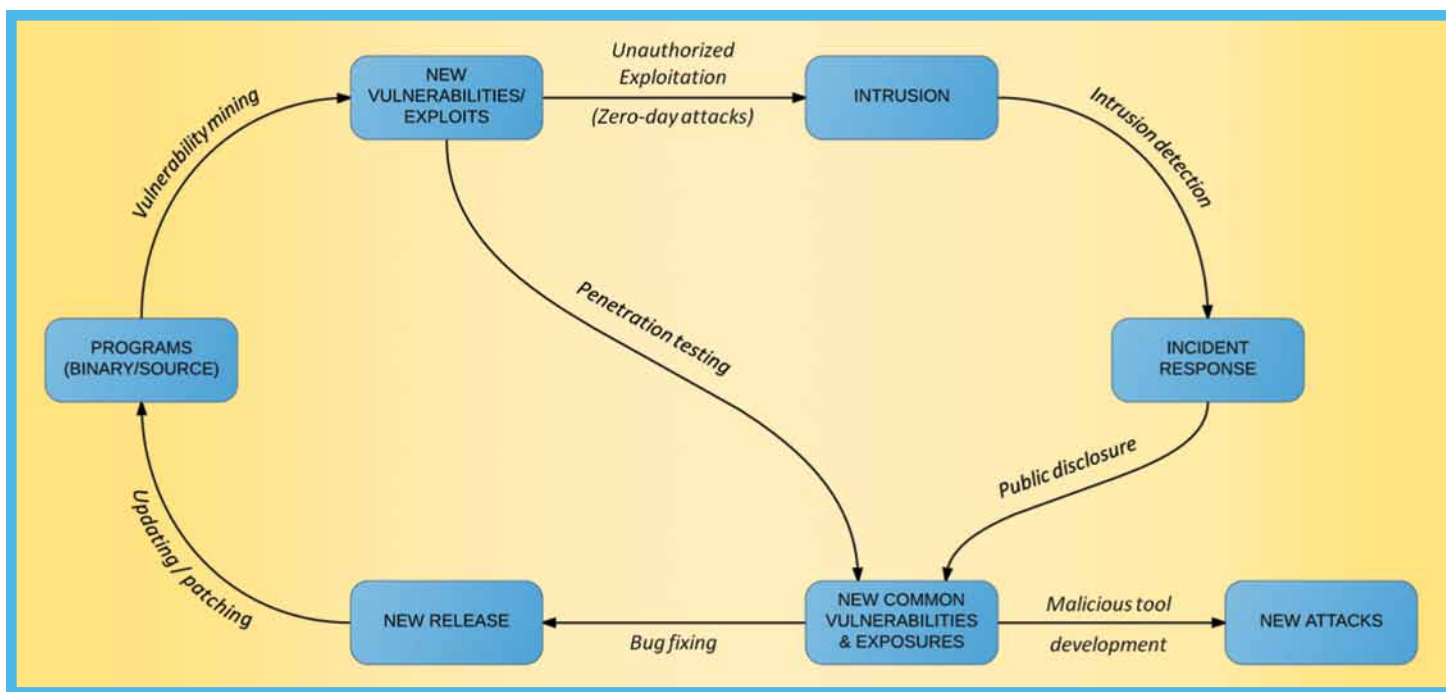
Disable inactive user accounts: Inactive user accounts are not maintained and can have vulnerable applications. Disable and remove them.

Document and track configuration changes: Document and track important configuration changes and review their performance.

Conduct vulnerability scanning and penetration testing regularly: Identify and fix vulnerabilities before attackers find them. Use vulnerability scanners continuously to examine the network and computers for known vulnerabilities. Perform penetration testing regularly.

Cyber Protection and Monitoring for Daily Activities

Log, filter, and monitor network system activities and programs to minimize network attacks and detect potential intrusions.



Life cycle of zero-day exploits. Image courtesy of the authors.

Check downloaded files against known viruses: Install up-to-date, anti-virus scanners on all computers and check all downloaded files.

Protect Ethernet ports and manage switches: Protect Ethernet ports and allow only authorized devices to be connected to ports. Use managed Ethernet switches to control network traffic.

Use and properly configure firewalls: Use a properly designed, secured firewall to control incoming and outgoing network traffic.

Use an intrusion detection and prevention system: Use an intrusion detection and prevention system (IDPS) to monitor network traffic and identify potential intrusions. Given the amount of network traffic, manual monitoring is impossible. However, the IDPS can be configured manually to protect against newly disclosed zero-day exploits when patches are not available.

Protect dial-in modems: Allow only authorized numbers for dial-in modems; remove them unless they are absolutely necessary.

Secure the wireless network: Allow only authorized devices to connect to the wireless network and monitor wireless activities. At seaports, connections from untrusted vessels could pose additional security threats.

Monitor public vulnerability disclosures: Monitor public vulnerability sites such as US-CERT (www.us-cert.gov/), ICS-CERT (<https://ics-cert.us-cert.gov/>), and software and

hardware vendors for new security disclosures. Patch all vulnerable systems and configure firewalls and IDPS systems to filter out exploit traffic.

Attack Surfaces and Attack Vectors

The attack surface of a system consists of its reachable and exploitable vulnerabilities. The smaller the attack surface, the smaller a port's risk exposure. A defense-in-depth system architecture takes into consideration these dimensions of the surface along with their sub-dimensions:

- **Network dimension:** The deployed network protocols (TCP/IP, IPv6, P2P, VPN).
- **Software dimension:** The software and interfaces, such as code, operating systems, configurations, web pages.
- **Human dimension:** The personnel and associated variables like social engineering, inside threats, errors, user naiveté.

An attack vector is a "point" on the attack surface for which the dimensions are specified. They are ways hackers can launch an attack, so they define an exploit's scope. Reducing the number of attack vectors improves system resiliency.

The Life Cycle of a Zero-Day Exploit

When an attacker uses a worm, virus, or other zero-day exploit, he or she opens a window of opportunity to do harm. From the seaport's perspective, that is the period of real vulnerability. The port closes that window when it successfully applies the appropriate patch.

The life cycle of a zero-day exploit has five stages:

1. A system is developed and deployed with an unknown vulnerability.
2. A hacker discovers the vulnerability before the developer does.
3. The hacker develops an exploit while the vulnerability is still unknown to the developer or, if known, not yet fixed.
4. The public becomes aware of the exploit either by independent discovery or by its use, and the developer releases a "signature" for the exploit.
5. The developer releases the fix/patch.

Incident Response

Establish steps and procedures to remove compromised components and restore systems in case of an intrusion. In the event that a seaport does not have its own incident response team, it should employ a certified cyber incidents service to handle incidents properly.

The Black Market

Black markets for trading exploits among hackers have existed since hacking began, and, as the effects of zero-day exploits grow, so does their value.

Recently, however, the markets for zero-day exploits are changing. For example, Microsoft recently paid \$100,000 to a hacking expert for a new exploitation technique.¹

Unfortunately, this provides incentive for more people to mine zero-day vulnerabilities and develop exploits. The interactions among these different players are likely to change the zero-day exploit economy.

Endnote:

- ¹ J. Finkle, "Microsoft awards hacking expert, repairs browser bug," www.reuters.com/article/2013/10/08/net-us-microsoft-cybersecurity-idUSBRE9970YK20131008.

Carefully establish incident response procedures: The team should follow the NIST incident response guidelines.⁶ Be sure procedures are structured, logical, and efficient to minimize impact to seaports. Preserve evidence such as logs and files for legal and liability issues.

Follow established procedures closely: Handling a security incident can be tricky, as attackers can use unknown tactics. Examine assumptions to avoid traps.

Contribute to a maritime information sharing and analysis center: Share information about incidents and responses via a maritime information sharing and analysis center.

Cyber Security Policy, Education, and Training

Enforce network and computer usage policies: Allow users to visit only trusted websites and use trusted applications. Since many cyber attacks require only one click on a malicious link or one visit to a malicious website, unlimited web browsing is inherently risky.

Provide regular cyber security training: Cybersecurity requires a collective effort. Users are the weakest link in security, as they are subject to social engineering, spear phishing, employing weak passwords, and malvertising. Stress cybersecurity and cyber awareness to all users and contractors. In addition, provide basic security protocol training.

Watch Trends, Boost Preparedness

As people have recognized the potential impact of zero-day attacks, government agencies, developers, and, unfortunately, malicious attackers, have driven up the dollar value for unpublished vulnerabilities. Increased demand has also led to increased activities in penetration testing and vulnerability discovery. In addition, zero-day vulnerabilities are often the critical first step in gaining access to systems. Terrorist and state-supported organizations will likely invest more on zero-day vulnerability discovery, resulting in even more zero-day exploits.

In particular, watering hole attacks⁷ via planted malicious software on targeted servers through zero-day exploits will also increase, since preventing such attacks requires additional business partner coordination and collaboration, creating further delays and barriers to securing the systems.

Along with increasing mobile device usage in businesses, zero-day attacks via mobile device vulnerabilities will increase as well. Mobile malware code increased from 792 in 2011 to more than 36,000 in 2012 and more than 50,000 in 2013.⁸ Therefore, it is important for seaports to have clearly defined policies for allowed devices on seaport networks.

A seaport is part of a complex maritime transportation system with many types of assets, operations, and infrastructure as well as a widely diverse set of stakeholders. These components share critical interfaces with each other and are often a part of a computerized network. The seaport security regime should likewise be built upon layers of protection and a defense-in-depth strategy that effectively mitigates critical system security risks, while preserving the functionality and efficiency of the seaport. All port stakeholders must work together to improve seaport cybersecurity awareness, mitigation, response, and recovery.



Any networked device associated with the seaport infrastructure is a potential zero-day vulnerability hotspot. U.S. Coast Guard photo by Petty Officer Tara Molle.

About the authors:

Mr. Xiuwen Liu is a computer science professor at Florida State University. His research interests include developing novel ways to secure cyber/physical systems and critical infrastructures and to detect zero-day exploits.

Mr. Mike Burmester is a computer science professor at Florida State University and director of the Center for Security and Assurance in IT. After more than 30 years of research and teaching, he joined the FSU faculty and has more than 120 publications on security topics, including privacy/anonymity, pervasive/ubiquitous systems, and cybersecurity.

Mr. W. Owen Redwood is a vulnerability researcher and Ph.D. student at Florida State University. He teaches students to find and disclose zero-day vulnerabilities in one of the nation's leading classes on offense/defense security. Owen's research interests are zero-day vulnerabilities, exploit development, critical infrastructure, and security visualization.

Mr. Fred Wilder, USCG Ret., spent 27 years as an officer in the U.S. Coast Guard. After being selected for Atlantic Area chief of staff, he retired to move into the commercial business world and currently works as a maritime technology and port security consultant.

Mr. Judd Butler holds an M.S. in educational psychology and learning systems from Florida State University where he worked for 10 years as an associate in research and project manager. He has 18 years of experience as an instructional designer and performance improvement consultant.

Endnotes:

- ¹ See <http://heartbleed.com/>.
- ² *Control Systems Security the Protection of National Infrastructure (CPNI)*. Available at http://ics-cert.us-cert.gov/sites/default/files/documents/Cyber_Security_Assessments_of_Industrial_Control_Systems.pdf.
- ³ L. Bilge and T. Dumitras. *Before we knew it: an empirical study of zero-day attacks in the real world*. Proceedings, CCS '12 Proceedings of the 2012 ACM conference on Computer and communication security, pp. 833–844, ACM, 2012. Available at <http://dl.acm.org/citation.cfm?id=2382284>.
- ⁴ Available at www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/SlickSheet_ApplicationWhitelisting_Standard.pdf.
- ⁵ NIST SP 800-63-2, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>.
- ⁶ K. Scarfone, T. Grance, and K. Masone. *Computer security incident handling guide*.
- ⁷ RSA Advanced Threat Intelligence Team, July 20, 2012, <https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/>.
- ⁸ McAfee Threats Report: First Quarter 2013. McAfee® Labs.

For more information:

US-CERT website
<https://www.us-cert.gov/>
 and
 ICS-CERT website
<https://ics-cert.us-cert.gov/>



Securing Your Control Systems

Overcoming vulnerabilities.

by MR. MATE J. CSORBA, PH.D.
Principal Engineer
Marine Cybernetics, Norway

MR. NICOLAI HUSTELI
Chief Technology Officer
Marine Cybernetics, Norway

MR. STIG O. JOHNSEN
Senior Researcher
SINTEF, Norway



Matthias Haas/iStock/Thinkstock

On a sunny day in August 2005, the IT staff at a Norwegian oil and gas company noticed suspicious network traffic through a firewall. At the same time, several personal computers (PCs) began behaving strangely. Engineers quickly identified the cause of the suspicious behavior—a malware computer worm.

The malware infected 157 hosts and affected 185 clients and servers. Investigators concluded that the malware infection, caused by a third-party PC connected to the internal network, could have consequences as far-reaching as a complete halt in offshore oil and gas production. Although it took a task force 50 hours to stabilize the network again, it was an incredibly lucky end to a cybersecurity incident, as there was no major impact.¹

Malware, or any other cyber attack, can occur on almost any system. For example, maritime control systems or navigation technologies are not immune to cybersecurity threats. Holes in cybersecurity have reportedly resulted in incidents such as tilting an oil rig off the coast of Africa, or bringing control systems to a standstill during relocation of a rig, due to malware infections.²

In July 2013, a team from the University of Texas at Austin successfully demonstrated GPS “spoofing” (sending false signals to a vessel navigation system) to change a vessel’s direction.³ Additionally, researchers from an anti-virus vendor demonstrated Automatic Identification System weaknesses, as they were able to shut down communication

between a ship and the port authority using a \$100 off-the-shelf radio kit.⁴

Recommendations and Guidelines

As control systems have incorporated more computerized remote operations, there has been a corresponding dramatic increase in the number of cybersecurity incidents, and the focus of these attacks has shifted from regular IT infrastructure to control systems. To address this issue, in June 2006, a Norwegian Oil and Gas Association workgroup published recommendations and guidelines for information security in industrial control and support systems and networks.

The association then conducted inspections in spring 2007, which uncovered discrepancies in network segregation,



Gigishots/iStock/Thinkstock

staff knowledge, and documentation, as well as confusion regarding the procedures to handle communication errors.⁵

In 2012, workgroup member, the Petroleum Safety Authority of Norway, released a self-assessment schema for vessel and rig owners operating on the Norwegian continental shelf, which covered cybersecurity topics grouped into 16 information security baseline requirements.⁶ Participants assessed their level of preparedness on a scale from zero to four (zero being the worst score). In the results specifically for drilling rigs, the overall average result was 2.4, with 1.5 being the worst score average on one of the information security baseline requirements.⁷

Ongoing Security Concerns

Unfortunately, an attack on a gas facility partially owned by the Norwegian state oil company in Algeria, in January 2013, showed that Norwegian interests in the oil and gas sector continue to be an attractive target for terrorist organizations.⁸

Additionally, one year later, the Norwegian National Security Authority's annual report listed 15,815 security incidents in national networks that year, 50 of which were

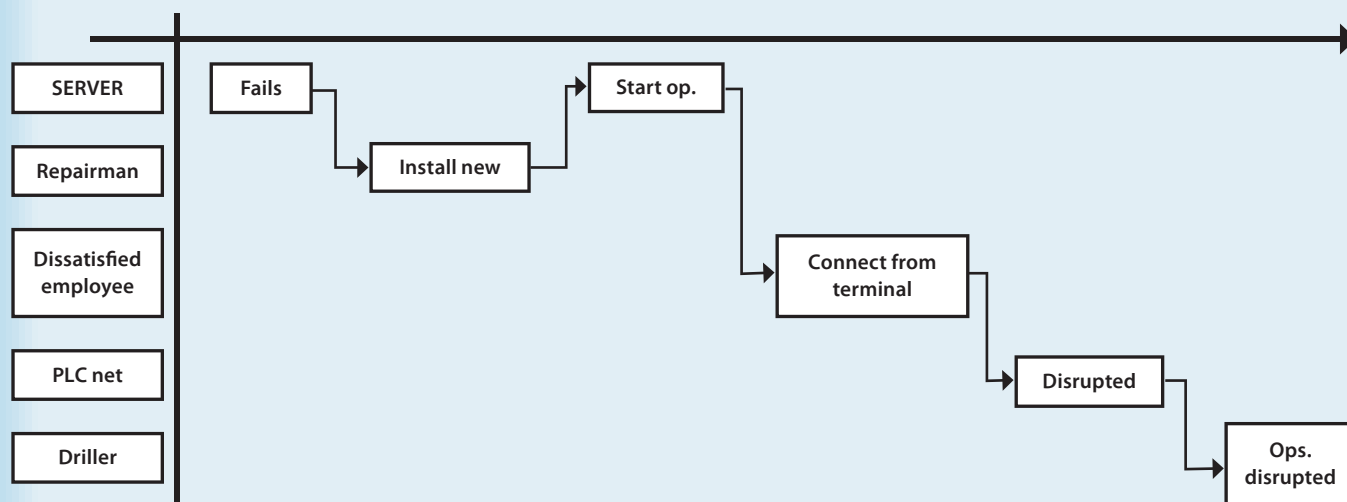
serious infiltration attempts against critical industrial networks (an increase from 46 in 2012 and 23 in 2011). The report concluded that enterprises lack awareness about their vulnerabilities, and while commercial security products are widely used, they are usually only capable of handling cybersecurity threats where the vulnerability is known beforehand. However, the report does suggest that third-party organizations could strengthen critical infrastructure and industrial communication systems cybersecurity.⁹

A Third-Party Approach

For example, hardware-in-the-loop (HIL) testing can be applied to verify functional correctness, failure-handling capabilities, and secure operations.¹⁰ Marine Cybernetics has been applying the HIL testing methodology since 2002 to test advanced marine control systems, such as dynamic positioning, power management, steering propulsion and thrusters, and blow-out prevention and drilling systems. We plan to complement this successful test approach by verifying cybersecurity.

In line with the guidelines from the Norwegian authorities, we have developed procedures for auditing cybersecurity and establishing an information security policy. For

Step diagram of a possible breach of network segregation on a vessel.



In this scenario, a driller's chair backup human/machine interface server fails irreparably and personnel replace it with a new computer. However, the server is connected to the drilling programmable logic controller network and the supervisory control and data acquisition network. A dissatisfied employee connects to the new backup server from an office terminal via remote desktop and accesses the programmable logic controller network to disrupt operations.

example, a sufficient information security policy document is approximately 10 to 15 pages and covers topics, including:

- security and safety policy definition, scope, goal, and strategy;
- scope and assets;
- supporting infrastructure security and safety;
- criticality assessment;
- security and safety related to third parties;
- information security organization, including roles and responsibility, operational procedures, security/safety training and awareness;
- security and safety requirements;
- critical system operational security;
- incident handling and management;
- disaster recovery plans.

Cybersecurity Auditing

To audit control system information security, we use an approach based on crisis intervention and operability analysis, which evaluates the control center personnel's ability to handle all modes of operation safely and efficiently. The method uses checklists and step-diagrammed scenarios to capture chains of events that will potentially lead to accidents or incidents and to identify critical mitigating actions.¹¹

Scenario walkthroughs can uncover critical decision mechanisms and verify personnel's ability to handle surprises and recover to normal operations. Moreover, the scenarios fill in

the gaps in information about the status of cybersecurity collected by going through custom checklists.

Vulnerability and Robustness Testing

While testing systems that provide open services and nodes in the telecommunication backbone (Web servers, routers, etc.) for vulnerabilities has a long history in cybersecurity research, supervisory control and data acquisition control system networks are new arenas for testing, and the focus has only recently shifted to critical infrastructure protection. Testing the communication networks serving human/machine interface systems and control systems often requires novel and custom tools, due to proprietary and closed-source solutions in contrast to the more open architectures such as the Internet.

Although various solutions exist, targeting known communication system vulnerabilities such as malware and virus scanners, vulnerability scanners, and intrusion-detection systems, they are severely dependent on updates or training. Therefore, it is equally important to scan communication systems for unknown vulnerabilities and to verify their robustness. A dynamic analysis method known as "fuzzing" can test communication protocol stacks in industrial control systems (ICSs) for unknown vulnerabilities. Fuzzing relies on "fuzzy" logic (a method that recognizes more than just "true" or "false" values) and seeks to trigger completely unexpected behavior in the software under test.

As testing software, such as communication protocols, in an entirely random way would be quite ineffective, state-of-the-art fuzzers combine techniques such as grammar rules that specify which parts of a protocol to fuzz, and various strategies for generating packets in an efficient way, systematically simulating invalid communication.¹²

Vendors often use remote login to provide support and use penetration testing to evaluate security and to determine whether there is proper network segregation. Appropriate segregation is key to properly seal off the control network from less critical networks, such as an office network. Network segregation is deemed insufficient if one can reach a probe installed in the critical part of the network from the other side of a segregation point.

Vendors also evaluate general ICS robustness by load testing and network “storm” simulation, where switches, devices, or controllers are flooded with network traffic to test how capable they are of handling the overload.

Maintaining the proper user rights is also paramount to limit unauthorized access to critical networks and control systems. For example, system personnel should forbid all types of access unless explicitly granted. They should also check for weak passwords, authorization bypassing, privilege escalation, and login locking.¹³

Moving Ahead

Today, an integrated approach for handling software and software updates is essential for successful vessel operations. Combining HIL testing and cybersecurity testing will increase maritime and offshore industry safety and security.

As threats to cybersecurity are increasing and appear from unexpected new angles, we believe that an up-to-date methodology is required to secure safe operations at sea. To maintain cybersecurity, it is beneficial to integrate testing into the change management cycle and establish a test strategy for all configuration changes and upgrades.

About the authors:

Mr. Mate J. Csorba is an electrical engineer, with a Ph.D. in telematics from the Norwegian University of Science and Technology, awarded for his research on optimization employing swarm intelligence. His professional background is in telecommunications, and he has worked for the Test Competence Centre of Ericsson, prior to joining Marine Cybernetics, where his focus is on communication systems.

Mr. Nicolai Husteli has worked with simulation technology for more than 13 years. He began his career at the Norwegian Marine Technology Research Institute as a research engineer. He joined Marine Cybernetics in 2006 and has been leading the development of the company's software platform for HIL testing. He has been the Marine Cybernetics chief technical officer since 2012 and has an M.S. in marine technology from the Norwegian University of Science and Technology.

Mr. Stig O. Johnsen is senior researcher at SINTEF, Norway.

Endnotes:

- ¹ R. Røisli (2006). HMS og IKT-sikkerhet i integrerte operasjoner (in Norwegian). Proceedings of a Ptil seminar 29.11.2006, Norway.
- ² J. Wagstaff (2014). All at sea: global shipping fleet exposed to hacking threat. Reuters.com.
- ³ Y. Dyravy (2014). *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*. NCC Group.
- ⁴ M. Balduzzi, K. Wilhoit, A. Pasta. *Hey Captain, Where's Your Ship? Attacking Vessel Tracking Systems for Fun and Profit*. 11th Annual HITB Security Conference in Asia, October 2013, Kuala Lumpur, Malaysia.
- ⁵ Recommended guidelines for Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems, Norwegian Oil and Gas Association, Jun 2006, revised Jan 2009.
- ⁶ Norwegian Oil and Gas Association recommended guidelines for Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems.
- ⁷ ISBR #1 – avg. score 1.9
ISBR #5 – avg. score 1.5
ISBR #7 – avg. score 1.9
- ⁸ The In Amenas attack, Statoil ASA investigation report. Available at <http://statoil.com>.
- ⁹ The Norwegian National Security Authority (NSM). Rapport om sikkerhetstilstanden 2014.
- ¹⁰ Korn, M. “In the Loop,” *Proceedings of the Marine Safety & Security Council, the Coast Guard Journal of Safety & Security at Sea*, Winter 2013-2014.
- ¹¹ The Crisis Intervention and Operability analysis method. Available at www.criop.sintef.no.
- ¹² Sutton, M., and A. Greene, P. Amini, *Fuzzing: Brute Force Vulnerability Discovery*. Addison-Wesley, 2007.
- ¹³ Authorization bypassing: Bad actors or others may try to “skip” authentication or logon pages by directly accessing internal page that is supposed to be available only after authentication has been performed. It is also possible to bypass authentication measures by tampering with requests and tricking the application into thinking that the user is already authenticated.
Privilege escalation is an attack against a system to access system resources that are normally protected.
Login locking is used to prevent brute-force, password-guessing attacks.

Building Port Resilience

How cyber attacks can affect critical infrastructure.

by Ms. APRIL DANOS
Director, Information Technology
Greater Lafourche Port Commission

America's ports face a seemingly endless list of urgent threats that range from acts of terrorism to energy supply security, and border protection, to drug and illegal weapons smuggling. While acknowledged as one of the most likely and potentially devastating threats of this new century, cybersecurity is often left off of the list of top threats to the port security community.

As a faceless, intangible threat to the security of our nation's ports, cybersecurity presents a much more complex and sinister danger to America's port security. Following a cybersecurity breach, vessels may be hijacked, pipelines ruptured, cameras blinded, and facilities left wide open.

Ports are designed to facilitate ingress and egress and efficient transit in, out, and through all manners of land, water, and even air interfaces. Moreover, major ports encompass a multitude of piers and other infrastructure, often spread over vast geographical areas, and their operations depend upon networks such as pipelines, roads, rails, and equipment that move goods, containers, and personnel to and from platforms, piers, and warehouses.

Port Resiliency

This makes port security a multi-faceted logistical challenge. In reality, the term "port security" does not correctly describe the real task: creating port resiliency—ensuring that, whatever happens, a port has the systems in place and the capacity to implement them properly, to prevent loss of life and property, and to return to normal operations as quickly as possible.

To do this involves:

- identifying critical assets and key resources for a port, on shore or at sea;
- assessing threats and vulnerabilities and the nature and extent of the damage or injury that may result;

- inventorying security assets and assets needed to recover from adverse events and positioning them to the greatest effect to deter, detect, respond to, and recover from activities that might prevent ongoing operations;
- inventorying infrastructure assets and hardening them to withstand likely events to ensure continued functionality through an adverse event or rapid recovery after an event;
- planning and training to maintain appropriate levels of readiness, skills, and experience to monitor ongoing operations and respond to and recover from adverse events;
- monitoring ongoing conditions to identify when adverse events occur;
- deploying resources to respond to and recover from adverse events, while monitoring the overall environment to maintain the big picture;
- establishing and maintaining reliable and secure communication channels to regional response partners and incident managers at local, state, and federal levels.

Technology

While this seems like a lengthy list of diverse tasks to juggle on a daily basis—much less during a crisis—port security professionals should take heart. The good news is that technology is available to help meet significant portions of the port resiliency challenge. Technologies for collecting and reporting information about the port's facilities and environment, for instance, have proliferated. Underwater sensors, surface and air radar, closed-circuit television, pressure-sensitive and other penetration alarms, GPS, equipment sensors, and a seemingly endless array of other devices are available in quantities and with capabilities that are limited more by the budget of the buyer than by the constraints of technology.

continued on page 40

C O M M A N D

The Port Fourchon Experience

As the southernmost port in Louisiana, with its prime position in the central Gulf of Mexico, Port Fourchon is the land base that provides support services to approximately 90 percent of all deepwater oil and gas activities in the gulf, including the Louisiana offshore oil port, the nation's only deep water oil port.

After 9/11 and Hurricane Katrina, the Greater Lafourche Port Commission (GLPC) members realized that the commission needed to bring security, emergency response, and operations into one common operating picture for greater situational awareness and interoperability with local, state, and federal agencies. So staff went looking for command and control solutions to allow the port to be more proactive than reactive.

In that search, GLPC members latched onto the concept of port-wide maritime domain awareness, and from that, Command, Control, Communications and Collaboration (C-4) was born. C-4 is designed to solve several business problems that Port Fourchon was facing in the early 2000s. These problems included:

- bringing security, resiliency, emergency response, and operations into one common operating picture for situational awareness and interoperability with local, state, and federal agencies;
- improving real-time collaboration with port tenants and local and regional first responders;
- creating a system that functions as an emergency response tool and can also be used daily;
- bringing together the port's disparate data systems;
- improving visibility across the port;
- enabling port harbor police to access this data in the field.

As GLPC personnel attempted to find solutions to these business problems, they knew that the ideal solution must:

- have a user-friendly interface;
- support daily operations, while using the emergency response application;
- leverage port security grant funding and meet national priorities;
- improve communications and situational awareness among the port commission, its tenants, and regional first responders beyond the port's geographic boundaries;

- leverage existing investments in technology where applicable and easily upgrade where necessary;
- improve understanding regarding the impact of a disaster through consequence analysis;
- monitor trends to allow users to better understand potential event escalation;
- provide mobile application support.

C-4

The C-4 system provides a visual, geospatially based portal that aggregates all sources of relevant data dynamically to build real-time situational awareness.

With all of these layers of data constantly available to port operators and peak law enforcement and emergency incident commanders, it is possible to monitor port weather, traffic, and water conditions in real time; investigate alarms remotely via interactive cameras; deploy messages to vessel and vehicular traffic; provide alerts of impending hazards to vessels; and assist response personnel.

The C-4 system also can be deployed on a video wall for emergency operations center support, or remotely from the Lafourche Parish government's emergency operations center building 50 miles inland.

How does it work?

GLPC's C-4 system was created on top of a commercial touch-assisted command and control system software package and leveraged the Department of Defense plug-in called the Knowledge Display and Aggregation System, which maps defense industrial base (DIB) assets, allows the operator to link external critical needs for those assets, add interactive vulnerability data, receive real-time threat data, and run on-the-fly threat assessments on potential DIB impacts.

There are multiple components to C-4, providing varying layers of access and functionality, and end-users are able to choose which layers they display.

Components include:

Integrated information: C-4 integrates information from individual data feeds and drops it in appropriate context into a single, dynamic display with a user-defined operating picture, or UDOP. The UDOP is geospatially organized, using satellite imagery, street maps, and other geospatially based reference material from a variety of sources.

Single interface: C-4 uses the UDOP as the single interface for all critical information and alerts, so the operator's attention is not constantly rotating among separate stovepipes of information located in independent computer screen windows.

Automated alert notification: The system continuously scans incoming alerts for those that indicate the possibility of a threat and then brings that threat to the operator's attention.

Interoperability: The system is designed to operate with all data feeds and other information sources, as well as with legacy software or new software.

Information sharing: C-4 incorporates role-based access controls and other technologies that enable seamless information sharing among different organizations, databases, and jurisdictions without revealing sources, methods, or confidential information that is not relevant to the operator.

Automatic status monitors: The system provides operator-defined status monitors that automatically keep track of the projected condition of individual assets, or individual missions, and indicate when the functionality of an asset or the completion of a mission is impaired.

Multiple response capability: Should an incident occur across multiple sites, the GLPC-C4 provides for multiple UDOPs that can be dedicated to response teams engaged in separate efforts.

Enhanced field coordination: C-4 enables the UDOP to become a common operating picture, showing all of the critical information available regarding the challenge in the field.

Simulation engine: Using the data derived directly from the operating picture, the user can recreate the existing circumstances in a simulation environment, simulate the effects in that environment of implementing a proposed response, and evaluate the projected effects of the proposed response against mission objectives.

Looking Ahead

GLPC members are in discussions with the U.S. Coast Guard to deploy C-4 with the Morgan City Maritime Safety Unit.

C O N T R O L



ongoing commitment to respond to a rapidly changing cyber threat environment.

So ports and other critical infrastructure assets conduct annual physical security exercises to ensure good working processes. Similarly, ports must conduct annual cybersecurity exercises that include law enforcement partners to ensure that they have appropriate notifications, forensics preservation, and investigation processes that meet the port's needs.

Port authorities and other critical infrastructure managers have ongoing relationships with federal partners to create and maintain physically secure environments. Similarly, any efforts to establish best practices or create a framework for managing cybersecurity must include a clearly defined role for the U.S. Coast Guard, which is the lead port security agency. Tasking the Coast Guard with responsibilities for cybersecurity within ports is logical, but will strain an agency that has already seen its mission and responsibilities expand greatly since 9/11. We would hope that any expansion of the USCG's role would be accompanied by additional resources to ensure that the agency can meet these new demands without compromising any of its other vital duties with respect to ports and the maritime industry.

Ports and other critical infrastructure managers have implemented physical security standards, hardening a key portion of the nation's border infrastructure against terrorism and crime. As the federal government works to ensure the cyber assets of these entities are similarly hardened, federal policy at all levels should consider how physical security goals and objectives can and should align with cybersecurity goals and objectives to best provide whole-of-asset security and resiliency.

How America's Ports Address Cybersecurity

The American Association of Port Authorities' information technology committee formed an information technology cybersecurity subcommittee in October 2013, consisting of personnel from several ports around the Americas who meet weekly to discuss cybersecurity and plan next steps to craft and implement policies that address emerging cybersecurity risks.

The subcommittee also provides comment and responds to requests for information in reference to cybersecurity, develops best practices, and maps future priorities for policy and legislation to better secure our nation's ports against cybersecurity threats.

Several ports have also participated in the Government Accountability Office's cybersecurity port review, and

Multiple communications technologies make it easy to transmit photos, text messages, and verbal reports about existing conditions. Simulation and modeling software programs can produce a plan for a building evacuation, and can produce portfolios of plans to fit a wide variety of circumstances dictated by a port's customary daily or monthly cycle of operations. On the response side, there are numerous software programs that address first responder operations.

Unfortunately, this massive proliferation of new technologies and their visible benefits have obscured the basic failure of technology to provide more effective tools to satisfy the most sophisticated demands of port resiliency. For instance, although there are a plethora of technologies available to gather information, there are fewer technologies that make it easier for port operators to understand exactly what all of this data means; and there are almost no technologies that enable port operators to tackle the challenges of implementing an operationally sound port resiliency plan. In other words, there is no technology capable of replacing port security professionals assessing data, putting it into proper context, spotting patterns, and making decisions to prioritize and protect people, property, and critical infrastructure in times of crisis.

How Cybersecurity Relates to Physical Security

Like physical security, which continually adapts to changes and new threat vectors, cybersecurity also requires an

others are working with local and federal law enforcement, as well as academic institutions, to identify and implement cybersecurity best practices.

Port information technology leaders, along with their counterparts in private industry, have confronted cybersecurity threats for some time. However, the issue of cybersecurity continues to grow in prominence and gain attention, evolving rapidly all the while, and there is a need for clarity in communication about goals, strategies, tactics, and objectives. To ensure that the federal government, state and local partners, and security experts are communicating clearly and efficiently, common language is critical.

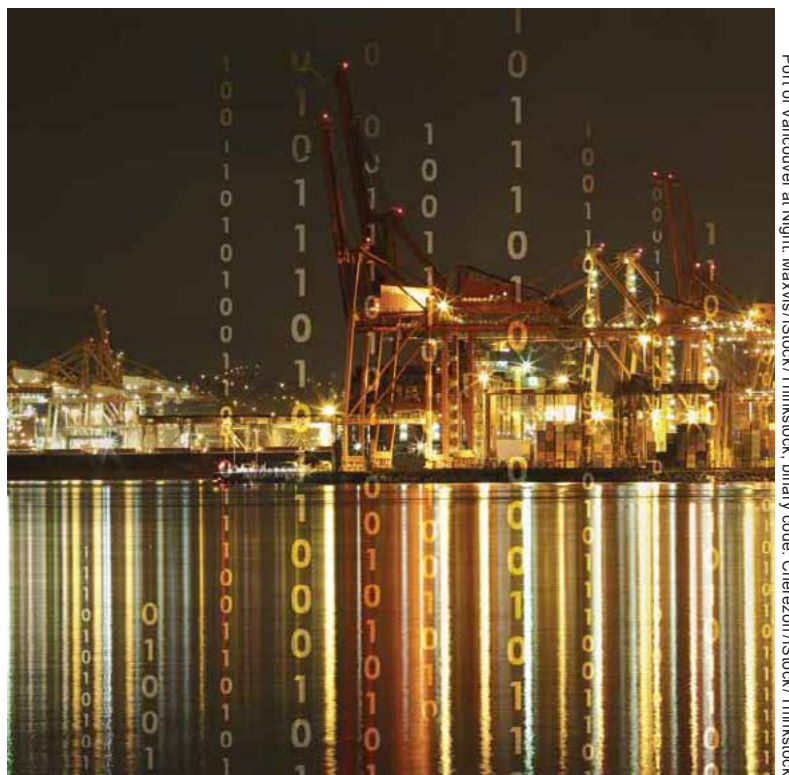
Maintaining Cybersecurity

While all of this new security technology makes us more prepared than ever for just about any hazard imaginable; if we are hacked, we are blind, useless, and potentially locked out of our own house. In essence, while technology helps us to be better prepared to contain and/or recover from any physical threats, it makes us more vulnerable than ever to cyber attacks, as we are utterly dependent on our technology for command and control of the port.

This makes cybersecurity more important than ever before and truly brings the physical and cyber threats to the same playing field. For example, think about what you could control remotely by technology a mere 10 years ago. What physical assets, access, cameras, systems, and such can you control remotely today in comparison? Imagine if someone else was controlling those assets and systems. What could they do? Sink a vessel in a channel? Turn off safety systems and pressure relief valves and structures on pipelines? Release hazardous materials stored on site? Lock personnel and vehicles in or out of facilities? Cut electricity, HVAC, telecommunications, and such to facilities?

With the stakes this high and the ability of today's cyber criminals and terrorists to take the smallest opportunities to do great harm to our port facilities, it truly takes every employee's efforts to maintain cybersecurity for our nation's ports and critical infrastructure assets.

Cybersecurity is everyone's responsibility, and little things add up to big things. From employees walking away from



Port of Vancouver at Night: Maxvix/iStock/Thinkstock; binary code: Cherezoff/iStock/Thinkstock

their desks without locking their computers, to plugging in and opening an unknown USB stick found in the parking lot, to working remotely in a dodgy Internet café to check email in Abu Dhabi, to loaning someone else their TWIC, or not vetting information technology (IT) contractors—cybersecurity risks are owned by more than just the IT department.

In short, port managers and our response partners across all levels of government need to remember and constantly remind our workforce that everyone has a vital role to play in continuing to provide layered cybersecurity to our ports and to the nation.

About the author:

Ms. April Danos is the director of Information Technology for the Greater Lafourche Port Commission. She is also the chairman of the information technology committee for the American Association of Port Authorities and chair of the IT cybersecurity subcommittee.

Maritime Critical Infrastructure Cyber Risk

Threats, vulnerabilities, and consequences.

by LCDR MARSHALL E. NEWBERRY
Inspections and Investigations Branch
U.S. Coast Guard 11th District

Imagine a maritime-based cyber attack causing kinetic effects or physical damage. In a worst-case scenario, such an attack could cause financial loss, terminal and/or port shutdowns, economic disaster, environmental catastrophes, and even loss of life.

Unfortunately, all of these consequences are possible and can certainly result from a large-scale cyber attack. So, to assess the probability of a cyber incident directed at any particular maritime industry component, we must first assess the risk of the incident.

Cyber risk is commonly approached as having three components, expressed algebraically as:

$$\text{Cyber Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}^1$$

Based on this definition of risk, if it were possible to eliminate any dimension completely, the resulting risk would also be completely eliminated. No vulnerability would mean there is no risk, despite the existence of a strong threat and severe consequence. Unfortunately, the likelihood of entirely removing any one dimension is marginal, if not impossible.

Cyber Threat Sources

According to the Industrial Control Systems Cyber Emergency Response Team, threat sources can be grouped into five main categories:²

1 National governments: National cyber warfare programs are unique and pose a threat to all U.S. interests. Among the current array of cyber threats, government-sponsored programs are capable of widespread, long-duration critical infrastructure damage. Unfortunately, some nation-states have the resources and commitment necessary for an attack to critical infrastructure. Their goal is to weaken, disrupt, or destroy the U.S.

2 Terrorists: Although terrorists, whose goal is to spread terror through the population, intend to damage U.S. interests, traditional terrorists are less developed in their cyber capabilities than are other adversaries. Therefore, terrorists are not likely to pose more than a limited cyber threat.

3 Industrial spies and organized crime groups: International corporate crime organizations pose a medium threat, as they can conduct industrial espionage, large-scale theft, and can hire and/or develop hacker talent. Their goals are typically profit-based and can include trade secret theft, attacks on competitors' infrastructure, and blackmailing affected industry regarding exposure threats.

4 Hactivists: This group is a small population of politically active hackers and includes individuals with anti-U.S. motives. They pose a medium threat of an isolated, but damaging attack. Their goal is to support their political agenda.

5 Hackers: Fortunately, hackers pose a negligible threat of widespread, long-duration damage to national infrastructure. Most hackers do not have the level of skill required to threaten U.S. critical networks and fewer have the motive to do so. However, because of the large population of hackers, the threat of isolated or brief disruption causing serious damage, including property damage or loss of life, is relatively high. However, with the growing number of skilled and malicious hackers, the likelihood of successful attack continually increases.

Vulnerabilities and Consequences

Since information technology has become the backbone of modern business and infrastructure, careful assessments of vulnerabilities and consequences of cyber attacks should be top priority. The Brookings Institute published a policy

Hack Attacks

Rig Tilt

Reuters reported that hackers were able to shut down a floating oil rig by tilting it. In a separate attack, a rig en route from South Korea to Brazil was so riddled with malware that its systems were brought to a standstill. It took 19 days of trouble-shooting and repairs to make it seaworthy again.¹

Aurora

On September 26, 2007, through an experiment dubbed "Aurora," researchers attempted to prove that a cyber attack could have kinetic effects. The experiment involved controlled hacking into a replica of a power plant's control system.

Researchers reportedly changed the generator's operating cycle, sending it out of control and destroying it. The intent was to assess vulnerabilities in the power grid that could cause physical damage to develop effective defenses.²

Stuxnet

In 2009 and 2010, the computer worm "Stuxnet," designed to attack programmable logic controllers (PLCs) in industrial control systems, destroyed nearly one-fifth of Iran's nuclear centrifuges at the uranium enrichment facility at Natanz.

Stuxnet reportedly compromised Iranian PLCs and forced the centrifuge's rotor to change speeds, inducing excessive stress and vibrations that destroyed the machines.³

Antwerp Attack

A cyber attack closely related to everyday U.S. container port operations took place in the port of Antwerp, Belgium, during a two-year period beginning in June 2011. A Dutch-based trafficking group hid cocaine and heroin among legitimate containerized cargo on ships originating in South America, then hired sophisticated hackers to infiltrate computer networks.

The breach allowed the hackers to access secure data, giving them the location and security details of the drug-laden containers. This allowed the traffickers to send drivers to steal the containers before the legitimate owners arrived.

The operation to hack the port companies reportedly happened in multiple phases, starting with malicious software being emailed to staff members, allowing the traffickers to remotely monitor company data. That initial breach was discovered and a firewall installed, after which hackers broke into the facility and fitted key-logging devices into computers,

which allowed them to gain wireless keystrokes and screenshots of staff workstations.⁴

The Shamoon Virus

On August 15, 2012, a cyber attack on the company Saudi Aramco infected 30,000 of its workstations with the self-replicating Shamoon Virus. Despite the company's vast resources, it took two weeks to recover from the attack.

While this attack did not result in an oil spill, explosion, or major operation shutdown, the attack affected business processes and drilling and production data were likely lost.⁵

Endnotes:

¹ Wagstaff, J. (2014). *All at Sea: Global Shipping Fleet Exposed to Hacking Threat*. Reuters. Available at www.reuters.com/article/2014/04/23/us-cybersecurity-shipping-idUSBREA3M20820140423.

² Meserve, J. (2007). *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*. CNN. Available at www.cnn.com/2007/US/09/26/power.at.risk.

³ Kushner, David. "The Real Story of Stuxnet". *IEEE Spectrum*.

⁴ Bateman, T. (2013). *Police Warning After Drug Traffickers' Cyber-Attack*. BBC News Europe. Available at www.bbc.com/news/world-europe-24539417.

⁵ Bronk, C., and Eneken Tikk-Ringas. (2013). *The Cyber Attack on Saudi Aramco*. *Survival: Global Politics and Strategy*. April-May 2013, Vol. 55, Edition 2.

paper in July 2013 documenting extensive research into gaps in critical infrastructure cybersecurity of U.S. ports, which revealed that the level of cybersecurity awareness and culture were relatively low among U.S. ports.³

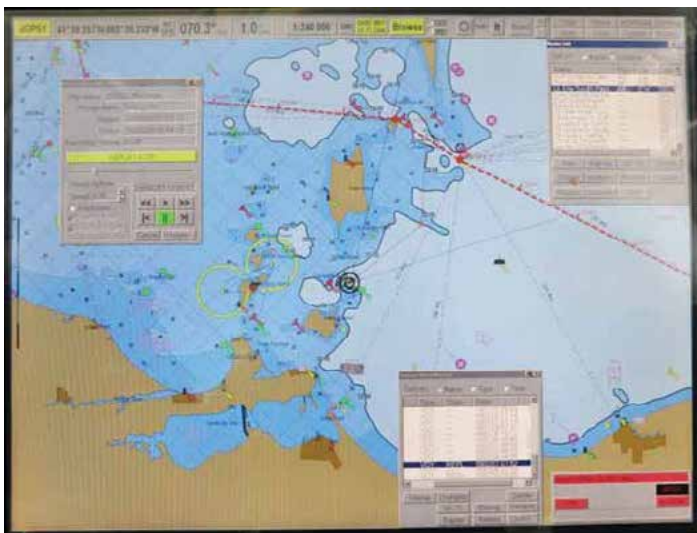
Although very few large-scale cyber attacks occur in the U.S., especially on maritime critical infrastructure, this is still important. Information gained from studying the large-scale cyber attacks of the past proves valuable to better understand some of the vulnerabilities and consequences to help calculate and reduce risk for today's operations.

All of these case studies can be applied to the maritime critical infrastructure, since today's marine terminal operations are moving more cargo faster, with fewer people and more automation. With port operations relying less on long-shoremen and more on automated systems, the opportunity

for cyber vulnerabilities and consequences have naturally increased.

Additionally, vessels themselves are also susceptible to cyber attacks. Navigation systems present a potential vulnerability. For example, researchers from the University of Texas recently demonstrated that a global positioning system (GPS) receiver could be duped by broadcasting counterfeit GPS signals (GPS spoofing) to present a set of false coordinates.⁴ Since modes, such as autopilot are reliant on GPS to guide the ship, this could result in devastating consequences.

The Automatic Identification System (AIS) is another potential source of vulnerability. A security software company found that AIS communications can be hijacked to create fake vessels and trigger false SOS or collision alerts. Other



An Electronic Chart Display and Information System. U.S. Coast Guard photo.

scenarios included injecting invalid AIS data such as position, course, speed, name, cargo, flag, etc., or creating and modifying aids to navigation entities.⁵

Finally, another well documented vulnerability is the vessel Electronic Chart Display and Information System (ECDIS), a computer-based navigation information system used as an alternate to paper nautical charts.⁶ While system use is generally restricted, the use of USB sticks, sensor infiltration, or intrusion into the vessel's local area network could cause them to be compromised. Vulnerabilities include access to modify ECDIS files and insert malicious content.

Cyber Defenses and Resources

The Brookings Institute Policy Paper provided a number of recommendations and conclusions to close the gap in cyber vulnerabilities. One highly underutilized program that all facilities should consider is the Federal Emergency Management Agency's Port Security Grant Program (PSGP). At the time of publication of the Brookings Policy Paper, the PSGP had appropriated more than \$2.6 billion, with only just less than \$6 million (or 2 percent) of those dollars going to directly fund cybersecurity projects. Given the national focus on cybersecurity, the PSGP is a highly recommended program for facility operators to pursue to fund cybersecurity projects.⁷

Additional recommendations include conducting cybersecurity assessments and response plans. Basic cybersecurity

hygiene needs to become fundamental. Companies should create a culture of awareness and incorporate procedures for strong passwords with consistent changes, prevent the connection of unknown devices and equipment to their systems, and develop education in common-sense practices. Such practices should include not clicking on unknown links or opening suspicious emails.

About the author:

LCDR Marshall Newberry is a U.S. Coast Guard Academy and University of Washington graduate. He holds a bachelor's degree and an M.S. in mechanical engineering. He has served the Coast Guard for more than 14 years, most recently in the 11th District Office of Inspections and Investigations, where he provides program oversight and has been instrumental in implementing Coast Guard cybersecurity initiatives throughout California, Arizona, Nevada, and Utah.

Endnotes:

- ¹ *Fed Approaches to Cyber Security* (2013). Available at www.fedcyber.com/fed-cyber-reference-library/federal-approaches-to-cyber-security.
- ² Industrial Control Systems Cyber Emergency Response Team. *Cyber Threat Source Descriptions*. Available at <http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>.
- ³ Kramek, Joseph, Commander, U.S. Coast Guard, Federal Executive Fellow. (2013). *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*. Center for 21st Century Security and Intelligence. Foreign Policy at Brookings. Available at www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek.
- ⁴ Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV. Available at www.ae.utexas.edu/news/features/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav.
- ⁵ Trend Micro Warns of Vulnerabilities in Global Vessel Tracking Systems. 2013 Press Release. Available at <http://apac.trendmicro.com/apac/about-us/newsroom/releases/articles/20131022085503.html>.
- ⁶ Dyravyy, Yevgen (2014). *Preparing for Cyber Battleships — Electronic Chart Display and Information System Security*. NCC Group. Available at www.nccgroup.com/en/learning-and-research-centre/white-papers/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security.
- ⁷ Kramek, Joseph, Commander, U.S. Coast Guard, Federal Executive Fellow. (2013). *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*. Center for 21st Century Security and Intelligence. Foreign Policy at Brookings. Available at www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek.

For more information:

The Coast Guard has developed a cybersecurity page on homeport. Access via www.homeport.uscg.mil and click on "cybersecurity" on the left side of the page. Additionally, a Homeport cybersecurity community has been developed for real-time information sharing. Directions for joining are on the Web page above.

Control System Cybersecurity

Legacy systems are vulnerable to modern-day attacks.

by LCDR JENNIFER M. KONON
Sector Intelligence Chief
U.S. Coast Guard Sector Delaware Bay

Maritime transportation system (MTS) operation is quite different than it was decades ago. Today's busy ports have become highly automated to handle the modern global market's demand for faster, more efficient shipping.

The Systems

Computer-based systems provide vital real-time information to operators, with supervisory control and data acquisition (SCADA) systems increasingly used to monitor and control a variety of functions, including valves in petroleum and natural gas pipes that transfer fuel between ships and shore and the gantry cranes that load and unload containers. Additionally, almost all modern cargo and U.S. military ships use SCADA systems in their sewage, propulsion, fuel, and fire-suppression systems.

Cyber attacks on these systems can threaten national security, economic stability, and public health and safety, so protecting such systems from cyber threats has become an issue of vital national importance.

The Vulnerabilities

Unfortunately, several system aspects make them especially susceptible to cyber attack. For example, most supervisory control and data acquisition systems in use today in the MTS are much older than other types of information technology (IT) systems. They were originally built as stand-alone systems and were designed before cybersecurity was a common consideration.¹

However, as computer and networking technology advanced, the demand for remote access to SCADA systems increased, which led to an often *ad hoc* integration of older supervisory control and data acquisition networks with newer corporate IT networks, creating hybrid networks. The decreased isolation of these systems increases vulnerabilities.

Today, many SCADA systems can connect to the Internet, which offers great convenience to operators, but also increases cyber vulnerabilities. More than one million of these systems are also discoverable on the Internet, with

What Makes SCADA Systems Tick?

The basic purpose of a supervisory control and data acquisition system is to allow remote control and monitoring, often for distribution systems such as transportation systems, natural gas and oil pipelines, power generation systems, and water distribution and collection. SCADA systems collect information from sensors on operating equipment, such as pumps, valves, switches, and sensors, then transmit and display the information to the end user in a geographically displaced location, allowing the user to

control and monitor the system in real time.

Several pieces of hardware make up the general structure—the human/machine interface, the master terminal unit, and the remote unit. The human/machine interface provides an interface between SCADA system commands and the user, the master terminal unit collects data locally, while the remote terminal unit receives the data from the master terminal unit and transmits

control signals to the field control systems that directly interact with the operating equipment.

SCADA system software allows the operating equipment to function within certain parameters and to initiate specific responses, should the equipment function outside of these parameters. For example, the system will open up pressure relief valves in a fuel transfer pipe if sensors indicate dangerously high pressure levels.

Attack Vectors and Attacks

Cyber threats may originate from a variety of actors, including disgruntled employees, criminals, hackers, nation-states, and terrorists, who may take advantage of the connectivity of these systems with Internet Protocol communications networks.

Threats

Once a virus or worm is introduced to a SCADA system network, it will propagate itself through networked control computers and disrupt communications to essentially prevent user control over the operating equipment. A Trojan horse (a malware program containing malicious code that can harm systems) may conduct damaging tasks, such as manipulating the system to make it more vulnerable to subsequent cyber attacks, or send false messages that cause undesirable control functions such as cycling valves or electric switches at the wrong times.

Consequences

Other cyber threats to SCADA systems exist irrespective of whether the system is connected to an IP network, including electronic communication threats such as radio frequency interference, electromagnetic pulse, and electromagnetic interference. These threats can greatly impact components' ability to

communicate with each other and properly send information between the operating equipment and the terminal units essential to monitoring and control.

A disruptive cyber attack on a system can also cause direct physical and environmental damage. For example, failure in a system controlling a gantry crane could cause a container to drop on workers below. Malicious manipulation of valves in a ship-to-shore fuel transfer system could lead to a devastating explosion on the pier or release pollutants into waterways. Any sort of disruption at a major seaport could cause significant disruptions in the global supply chain, affecting the shipment of essential goods, and cost billions of dollars.

Defense-critical infrastructure also relies on SCADA systems. An attack would affect the nation's defensive capabilities and thus national security, and the interdependency of MTS components and other infrastructure nodes could cause grave national and global consequences.

Attacks

Sadly, some of the possible scenarios have come to fruition. In 2000, a man rejected for employment at an Australian

sewage plant used a laptop and radio equipment to issue commands to the plant's SCADA system, causing millions of gallons of untreated sewage to be dumped into rivers, parks, and other surrounding properties.¹

In 2010, the Stuxnet worm damaged Iranian industrial sites, including a nuclear plant. The worm traveled easily across systems linked to the Internet, and was introduced to isolated systems by simple human error, most likely via USB drives.²

Finally, an unintentional disruption of critical valve operations at water, electric, and gas companies, caused by electromagnetic interference from a U.S. Navy radar system, showed how even benign sources can interfere with vulnerable supervisory control and data acquisition systems.³

Endnotes:

¹ Weiss, *Protecting Industrial Control*, p.p. 108-109.

² *Hearing before the House of Representatives Subcommittee of National Security, Homeland Defense and Foreign Operations of the Committee on Oversight and Government Reform, Cybersecurity*, 26; David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, Feb. 26, 2013.

³ US-CERT Control Systems Security Center, *Cyber Incidents Involving Control Systems*, Robert J. Turk, INL/EXT-05-00671 (October 2005): p. 32.

their unique Internet Protocol addresses.² A 2005 report to the U.S. Congress estimated that Internet-connected supervisory control and data acquisition systems were probed by hackers on a daily basis.³

Further, the commonality of various types of SCADA components, from software to hardware, raises the potential impact of a cyber attack. Newer systems often use commercial off-the-shelf technologies, and providers often publish standards for interconnection, alarm communication, and other types of control. Cyber attackers may take advantage of this information. Many of these systems come with a significant amount of interdependency and little isolation across multiple modes. Therefore, a cyber attack on a terminal management system could also affect aspects of connected truck, rail, and maritime transportation.

A final significant contributor to SCADA systems' cyber vulnerabilities lies in the human factor. Employees may introduce cyber vulnerabilities by using poor security practices, such as choosing weak passwords or allowing unauthorized personnel access.

Risk Mitigation

To mitigate cyber threats, IT personnel should conduct risk assessments and improve security policy training and enforcement. They should also eliminate any unnecessary connections between SCADA networks and other networks, and fortify necessary network connections, using measures such as firewalls at every point of entry.

If organizations use commercial off-the-shelf supervisory control and data acquisition systems, personnel should

disable any unnecessary or unused network services. Finally, IT personnel must implement strong authentication for any systems used for maintenance or communications, whether they be wired, wireless, or modems, lest they be used as a “back door” to infiltrate a SCADA network.

Government Efforts

The U.S. government is taking an aggressive approach to promote SCADA system cybersecurity in the nation’s infrastructure, including the MTS. Department of Homeland Security (DHS) personnel created a control systems security program and a cybersecurity evaluation tool to help industry owners assess and improve their cybersecurity posture. DHS also provides onsite security consultation specifically targeted at SCADA systems.

Additionally, the U.S. Coast Guard is raising awareness regarding such resources for MTS owners and operators, and highly encourages MTS personnel to review and implement recommendations made in the National Institute of Standards and Technology cybersecurity framework (see related article).

Unfortunately, bad actors, ranging from criminals and terrorists to disgruntled employees, may wish to tamper with SCADA systems, and the means for them to do so are becoming more sophisticated. MTS leaders and the U.S. government must continue to take these threats seriously and enforce measures to enhance the cybersecurity of these crucial systems.

About the author:

LCDR Jennifer Konon is the chief of the Intelligence Division, U.S. Coast Guard Sector Delaware Bay. She is a 2002 graduate from the U.S. Coast Guard Academy, and holds a bachelor’s degree in government and a master’s degree in astronomy. She has served on the Commandant’s Intelligence Plot and is currently a candidate for a master’s degree in science and technology intelligence with a cyber concentration at the National Intelligence University.

Endnotes:

- ¹ ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure, U.S. Department of Transportation, July 2013.
- ² Cyber Security for SCADA Systems, Thales Group, Autumn 2013.
- ³ Cai, N., Wang, J. and Yu, X. (2008). SCADA system security, p. 569.

Bibliography:

- Henrie, M. “Cyber Security Risk Management in the SCADA Critical Infrastructure Environment.” *Engineering Management Journal*, no. 25.2, June 2013.
- Stouffer, K., Joe Falco and Karen Scarfone. *Guide to Industrial Control Systems Security*, National Institute of Standards and Technology, NIST Special Publication, 800-82, rev. 1, May 2013.
- Hentea, M. “Improving Security for SCADA Control System.” *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 3, 2008.
- Hart, D. *An Approach to Vulnerability Assessment for Navy Supervisory Control and Data Acquisition (SCADA) Systems*. Naval Postgraduate School, master thesis, 2004.
- Amanullah, M.T.O., A. Kalam and A. Zayegh. *Network Security Vulnerabilities in SCADA and EMS*. Transmission and Distribution Conference and Exhibition, Asia and Pacific, 2005 IEEE/PES.
- Creery A. and E.J. Byres. *Industrial Cybersecurity for Power System and SCADA Networks*. Amaroso, Cyber Attacks, 62-63; Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual.
- Cai, N., Jidong Wang and Xinghou Yu. *SCADA System Security: Complexity, History, and New Developments*. Industrial Informatics, 2008 6th IEEE International Conference on Industrial Informatics.
- Kramer, F.D., Stuart H. Starr and Larry K. Wentz. *Cyberpower and National Security*. Washington, D.C.: National Defense University Press, 2009, p. 128.
- ICS Security in Maritime Transportation. *A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure*. U.S. Department of Transportation, July 2013.
- National Institute of Standards and Technology. *Guide to Industrial Control Systems Security*, 2-6.
- Weiss, J. *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum Press, 2010, p. 44.
- National Strategy for Maritime Security*. Washington, DC: The White House, National Maritime Domain Awareness Plan, December 2013.

Hide and Seek

Managing Automatic Identification System vulnerabilities.

by LCDR ALLISON MIDDLETON
Intelligence Division Chief
U.S. Coast Guard Cyber Command

Ships use the Automatic Identification System (AIS) to identify and track other ships to prevent a collision, provide vessel description, information on the next port of call, and such. AIS also aids vessel traffic services, provides maritime domain awareness, supports search and rescue tracking, enables fleet monitoring, allows aids to navigation location transmission, and can assist in mishap investigations.

Exploiting Weaknesses

However, the system has vulnerabilities that bad actors can exploit. Criminals or other adversaries can use these weaknesses to create fictitious vessels, make vessels “disappear,” or change a ship’s location or characteristics.¹

These tricks may allow bad actors to evade law enforcement or national security measures to smuggle drugs, money, or even weapons of mass destruction. Even the unintentional

AIS Vulnerabilities

AIS Websites

AIS websites rely on the Internet to transmit information to commercial websites and to the U.S. Coast Guard. However, commercial providers do not always use the best information security techniques to protect their data.

Therefore, displayed information is only as secure as the network it is connected to. If someone or something compromises the network, much of the legitimate data sent to the commercial providers could be altered, including position, course, cargo, flagged country, speed, name, and Mobile Maritime Service Identity status.

A network intrusion could also allow a criminal or adversary to create a fake vessel with the same details in another location. Aids to navigation information is also displayed on these commercial sites, and a cyber attack into a network could allow an adversary or criminal to change the location and other identifying information related to an aid to navigation.

Radio Frequency Transmissions

AIS radio frequency (RF) transmissions are not secure. There are no validity checks, timing checks, or authentication. Therefore,

spoofing Automatic Identification System RF transmissions is possible, but it requires the bad actor to purchase an AIS base station, develop an original AIS transmitter, or exploit an existing transponder and control it to transmit unauthorized messages.

Therefore, criminals or adversaries could take advantage of the lack of secure transmissions to disable an AIS system on a vessel; trigger a distress beacon that will also trigger alarms on all vessels within approximately 50 km; or create a fictitious collision warning alert. The last scenario is probably the most troubling, because some vessels have software that will automatically recalculate and change their course, based on collision alerts.

Denial of Service

AIS is also vulnerable to a “denial of service” attack (an interruption in an authorized user’s access to a network, typically one caused with malicious intent).

Insecure RF signals could allow a criminal or adversary to spoof an AIS signal that would cause all ships to send AIS information much more frequently, which would result in a denial of service attack on all vessels in close proximity.

AIS misuse could have a negative impact to maritime safety, such as obscuring the location and identification of a vessel involved in a search and rescue mission.

Incidents

Criminals have attempted to evade law enforcement by misusing the Automatic Identification System. In April 2010, an Argentinean Coast Guard vessel intercepted a fishing vessel illegally operating one mile inside Argentina's exclusive economic zone. The vessel attempted to evade the Argentinean Coast Guard by sailing into international waters and disconnecting its AIS equipment.²

In another example, researchers associated with a software and cloud computing security company demonstrated how an adversary could hijack AIS information and perform attacks that enable them to turn the tracking system into a liability by "spoofing" information going from a ship's AIS to online tracking services.³ This type of control can allow a bad actor to change a vessel's reported location and alter characteristics, including size, type, origin, or even cargo.

Mitigation

While most mariners know about and tolerate AIS vulnerabilities, possibly the best way to mitigate most of its vulnerabilities is to use more than one system to identify vessels.

For example, long-range identification and tracking (LRIT) is a maritime security system that utilizes more secure transmitters—as opposed to AIS—which serves primarily maritime safety purposes. When mariners use both LRIT and AIS in conjunction, anomalies become more apparent that could indicate criminal or adversarial compromise of either system.

Moreover, the U.S. Coast Guard uses the authoritative vessel identification service to collect data from many different databases to verify a vessel's identification. This method helps identify erroneous data or anomalies. Also, time difference of arrival is another possible mitigation technique that could more closely authenticate vessel location, by calculating the time it takes for a single AIS transmission to reach multiple land-based antennas.

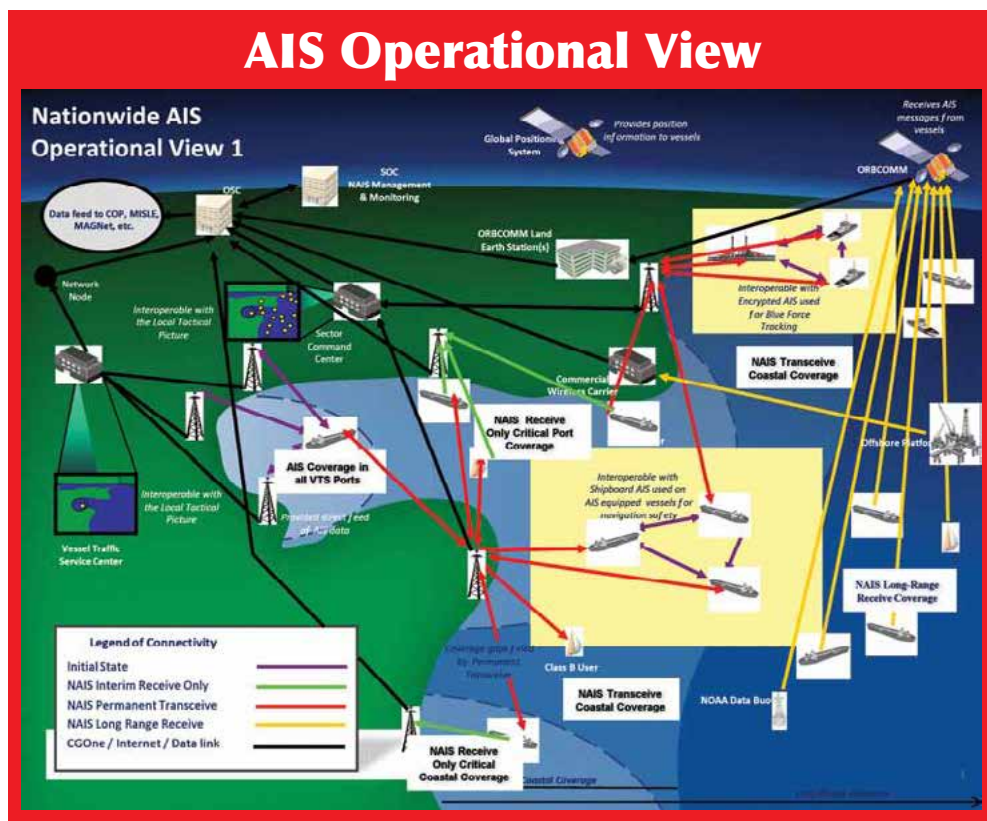


Image courtesy of U.S. Coast Guard NAVCEN.

Finally, even though AIS's network, transmitters, and commercial websites that display its data are all vulnerable, mariners can mitigate vulnerabilities by using multiple systems/techniques to validate their ship's location and identify ships in close proximity.

About the author:

LCDR Allison Middleton is the Intelligence Division chief at Coast Guard Cyber Command. LCDR Middleton has served in the USCG in a variety of operational, training, and intelligence billets since her 2003 graduation from the U.S. Coast Guard Academy. She has an M.A. in intelligence analysis, an M.S. in human performance improvement, and an M.E.D. in curriculum and instruction.

Endnotes:

¹ The Guys Who Can Make Oil Tankers Disappear, Virtually. ABC news, October 2013. Available at <http://abcnews.go.com/Blotter/guys-make-oil-tankers-disappear-virtually/story?id=20565851>.

² Argentine Coast Guard Arrest Korean Jigger for Illegal Fishing. Merco Press, April 30, 2010.

³ ABC news.

Bibliography:

Researchers highlight security vulnerabilities in ship tracking system. Dark Reading, Oct. 13, 2011.

Vulnerabilities Discovered in Global Tracking System. Washington, DC: Department of Homeland Security, Weekly Analytic Synopsis Product, Oct. 18, 2013.

The Truth about AIS Spoofing: Web-Based Tracking Vulnerable, but... Written by Jeff Robbins, PassageMaker, Oct. 27, 2013. Available at www.passagemaker.com/articles/trawler-news/the-truth-about-ais-spoofing-web-based-tracking-vulnerable-but/.

GPS Spoofing and Jamming

A global concern for all vessels.

by Ms. BRITTANY M. THOMPSON
Analyst
Former Detailee at U.S. Coast Guard Cyber Command

Picture yourself driving and following directions from your Global Positioning System (GPS)-enabled device to a place you have never visited. Along the way, you realize that you have reached a totally different destination. Now, imagine this same scenario, but instead involving a vessel sailing off course, while at sea. How could this possibly happen? Two words: GPS spoofing.

Spoofing

GPS spoofing is an electronic attack involving signals being sent to a receiver to control navigation. This act could force any mode of transportation to deviate from its intended route.

This type of attack is insidious, since Global Positioning System data is used to direct traffic through busy waterways to reduce accidents and avoid hazards. It also helps manage shipping and port facility operations. For example, Global Positioning System information facilitates automated container shipment and tracking from one port to another.

At the Coast Guard, GPS is the primary mode of navigation for its cutters and other assets. So, it is critical that location and positional data from a Global Positioning System-enabled device is accurate, to ensure vessels safely and efficiently carry out missions and reach their destinations.

Incidents

The Disruption at Newark Airport Was Unintentional

A truck driver for an engineering company allegedly used a jammer in a company-owned vehicle to hide his whereabouts from his employer. Since his driving route took him past the airport, the jammer not only blocked reception of the company-installed Global Positioning System signal, but also the airport's GPS signal used by air traffic control.

The FCC's Enforcement Bureau investigated the incident and used radio monitoring equipment to detect the suspect's jammer in use near the airport. As a result, the suspect surrendered the jammer and the FCC fined him nearly \$32,000 for disrupting Newark airport's GPS signals.¹

North Korean Jamming Attacks

Interfering with GPS signals is a capability used against other nations by its adversaries. For example, North Korea perpetrated three GPS jamming attacks against South Korea from 2010 to 2012.²

Each jamming attack increased in duration. The first attack in August 2010 lasted for four days. The last attack in 2012 lasted for 16 days, causing 1,016 aircraft and 254 vessels to experience interruption.³

Overall, the jamming attacks resulted in major issues associated with navigation and timing in the areas near the North Korean border. Additionally, an attack necessitated an emergency landing of a U.S. military reconnaissance aircraft, during an annual exercise in South Korea.⁴

Endnotes:

¹ Strunsky, S. N.J. *Man Fined \$32K for Illegal GPS Device That Disrupted Newark Airport System*. NJ.com. N.p., 8 Aug. 2013.

² Available at www.economist.com/news/international/21582288-satellite-positioning-data-are-vital-but-signal-surprisingly-easy-disrupt-out.

³ Ibid.

⁴ Available at www.insidegnss.com/node/3982.

Jamming

GPS jamming, where a bad actor blocks Global Positioning System signal reception, is related to spoofing. For the maritime environment, jammers are a threat, because they deprive a vessel of the capability to determine its true position at sea. Moreover, without this capability, a vessel cannot broadcast its location to others through systems such as the Automatic Identification System.

Additionally, criminals and terrorists can use jammers to aid in their illicit activities and evade law enforcement by hiding their location.

Mitigation

Despite much research and improvements in antenna and receiver design and experiments with signal authentication, the fact remains civil Global Positioning System signaling is unencrypted; only military GPS signaling is encrypted for use in smart weapons technology.¹

However, some non-satellite-based alternatives are available for navigation to mitigate the risk of GPS disruptions. For example, eLoran (enhanced long range navigation) is an advanced version of the old Loran-C land-based radio navigation system. The new system uses high-powered signals over low frequencies and reportedly accurately maps destinations within 10 meters.²

Further development of alternate non-satellite-based navigational tools to reduce Global Positioning System dependence would be worthwhile. In addition, non-satellite-based tools will enable continuity of operations in the event of a disruption or outage. It is also important to encourage continued technological advancements for GPS receivers, so it will become more difficult to interfere with or block the signals.

Future Focus

The benefit of using Global Positioning System information in a wide variety of applications has definitely come at a cost to society. In instances when a GPS system is tampered with either purposefully or accidentally, those actions will

NAVCEN

In 1988, the Coast Guard became the operational interface for public and private users of GPS, so GPS spoofing is of particular concern to the Coast Guard.

“Directionally, spoofing will make a boat think it’s going in the right direction but it’s actually off track,” says the Coast Guard Navigation Center’s (NAVCEN) Rick Hamilton, who is also the executive secretariat for the Civil GPS Interface Committee.

NAVCEN personnel operate services and manage Coast Guard navigational

matters, including liaison duties for civil GPS operations and reports of GPS outages or interference.

As Hamilton describes, “We help provide a coordinated government response to reports of interference. We review, triage the report, and then try to get someone in the area to determine if there really is an issue. If so, we work with partners at the FAA, Air Force, and the FCC Enforcement Bureau to find the source of the event and stop it.”

impact other systems. Therefore, GPS spoofing and jamming are considered cybersecurity threats of concern to not only the maritime industry, but to the transportation sector as a whole.

About the author:

Ms. Brittany M. Thompson is an analyst and a former detailee at Coast Guard Cyber Command. She has an interest in cyber intelligence and cybersecurity topics. In 2013, she completed a joint master’s and MBA in cybersecurity at the University of Maryland–University College.

Endnotes:

¹ Warner, Jon S., Ph.D., and Roger G. Johnston, Ph.D., CPP. *GPS Spoofing Countermeasures*.

² *No Jam Tomorrow*. The Economist, March 12, 2011.

Bibliography:

CGSIC General Information. U.S. Coast Guard Navigation Center, March 19, 2014.

Gibbons, G. *Republic of Korea Announces New Plan for eLoran System in Wake of GPS Jamming*. Inside GNSS. Global Navigation Satellite System Community, Gibbons Media & Research LLC., April 14, 2014.

GPS Jamming: Out of Sight. The Economist. The Economist Newspaper, May 16, 2012.

Interview with the U.S. Coast Guard Navigation Center’s Rick Hamilton. Telephone Interview, April 2, 2014.

Marine. GPS.gov: Applications. National Coordination Office for Space-Based Positioning, Navigation, and Timing, Sept. 27, 2013.

No Jam Tomorrow. The Economist. The Economist Newspaper, March 12, 2011.

Strunsky, S. N.J. *Man Fined \$32K for Illegal GPS Device That Disrupted Newark Airport System*. NJ.com. N.p., Aug. 8, 2013.

Warner, Jon S., Ph.D., and Roger G. Johnston, Ph.D., CPP. *GPS Spoofing Countermeasures*.

Department of Homeland Security Efforts

Implementing cybersecurity initiatives throughout the federal government.

by LCDR MAUREEN D. JOHNSON

Port and Facility Activities Section Chief

U.S. Coast Guard Pacific Area Prevention Operations Planning Staff

Cybersecurity is not a new concept. For as long as computers have been interconnected, information technology managers have fought to keep networks and data secure. However, as industrial control systems and other maritime transportation system (MTS) technologies become increasingly networked, the increased efficiency comes with a cost—cybersecurity vulnerabilities that transcend the typical physical security maintained within our ports.

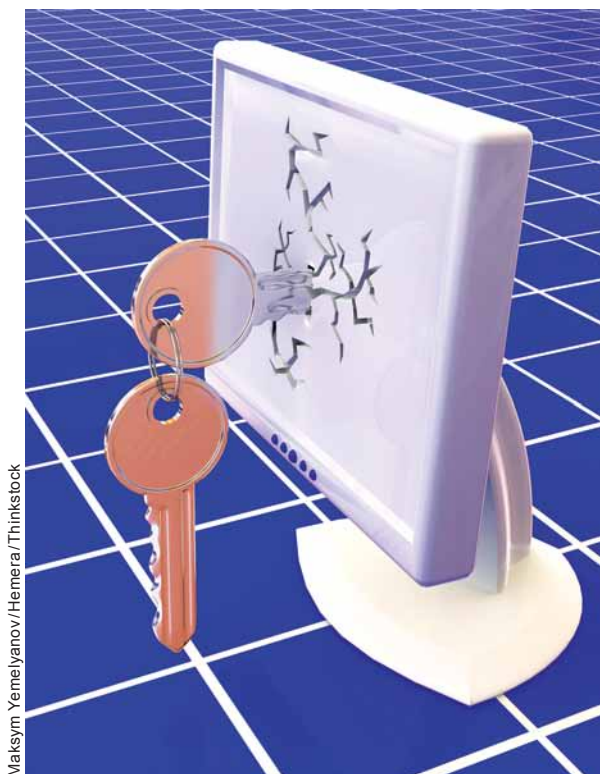
Government efforts to defend against these risks include the Department of Homeland Security (DHS) National Infrastructure Protection Plan, which taps the Coast Guard as the sector-specific agency for the maritime mode of transportation.¹ It is in that role that the USCG is working to identify risks, develop policy, and strengthen intra-governmental and industry partnerships and information sharing networks to promote maritime sector cybersecurity.

MTS Cybersecurity and Information Sharing

Within the Coast Guard, numerous entities have a direct interest in MTS cybersecurity. For example, sectors, marine safety units, and marine safety detachments are the primary interface with the maritime industry and are the most familiar with facility and vessel physical layouts, cargoes, and existing physical security measures.

Captain of the port² (COTP) authority and the responsibilities of the federal maritime security coordinator³ (FMSC) reside primarily at the sector level. In terms of security and cybersecurity, the FMSC typically chairs or co-chairs the area maritime security committee (AMSC). While committees vary among ports, they are generally comprised of federal, state, local, and tribal government representatives; port, company, and facility security officers; trade representatives; and marine exchange representatives. The members' varied responsibilities, experiences, and backgrounds contribute greatly to developing local action plans that address cybersecurity risks.

Additionally, information regarding cybersecurity, emerging threats, and cybersecurity best practices are all shared as appropriate at the AMSC meetings. Sector personnel regularly interface and share information with industry through various formal and *ad hoc* committees and meetings such as



Traditional physical security protocols do not even begin to address cybersecurity threats.

harbor safety committees, industry trade association meetings, and other specialty or local groups.

Within Coast Guard headquarters, the Office of Port and Facility Compliance is the lead for MTS cybersecurity, and personnel oversee preparedness activities aimed at preventing, responding to, and recovering from hazards that could have a destabilizing effect on the nation's economic strength, public health, safety, and homeland security.

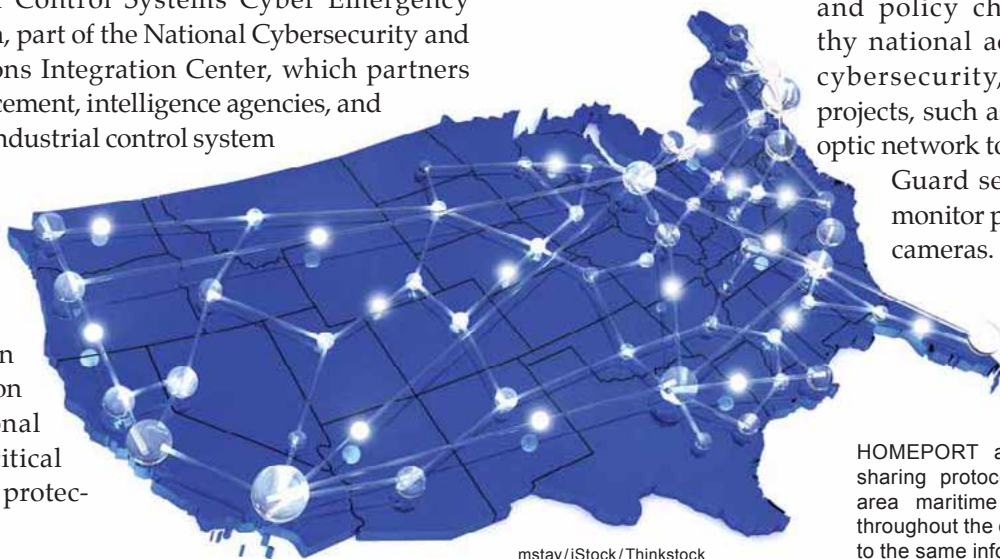
CG Cyber Command has subject matter experts who have experience in MTS critical infrastructure cyber threats and vulnerabilities. Additionally, CG Cyber Command personnel identify and disseminate cybersecurity threat information and best practices to operational commanders and maritime partners.

Information Sharing Among Federal Agency Partners

The Department of Homeland Security is the lead department that implements cybersecurity initiatives throughout the federal government. Within DHS, the lead office is the Directorate for National Protection and Programs, which includes the Office of Infrastructure Protection and the Office of Cybersecurity and Communications.

There are also numerous offices, command centers, and working groups within DHS that are or will be part of the larger whole-of-government coordination effort to address cybersecurity incident prevention and response, including:

- the Homeland Infrastructure Threat and Risk Analysis Center, a joint fusion center of the Office of Infrastructure Protection and the Office of Intelligence and Analysis;
- the United States Computer Emergency Readiness Team, the 24-hour operational arm of the National Cybersecurity and Communications Integration Center;
- the Industrial Control Systems Cyber Emergency Response Team, part of the National Cybersecurity and Communications Integration Center, which partners with law enforcement, intelligence agencies, and private sector industrial control system users;
- the National Infrastructure Coordinating Center, the information and coordination hub of a national network for critical infrastructure protection.



mstay/iStock/Thinkstock

Additionally, the Coast Guard is leveraging partnerships with other homeland security agencies such as Customs and Border Protection and Immigration and Customs Enforcement, as well as the FBI, to develop cybersecurity initiatives.

FBI personnel are also engaged at the individual port level, interacting with USCG and port partners through AMSCs and other industry and law enforcement working groups. For example, the FBI has field office cyber task forces that focus exclusively on cyber threats.

The Coast Guard is also forging new partnerships, such as with the Department of Energy (DOE). Coast Guard leaders recognized the significant potential for the DOE's Cyber-Security Capability Maturity Model (C2M2) to be modified and utilized within the maritime sector. DOE personnel initially developed the C2M2 for the electricity sector to better protect the nation's electrical grid. The tool helps organizations evaluate, prioritize, and enhance cybersecurity capabilities, so it is expected that collaboration with DOE will allow Coast Guard personnel to integrate DOE lessons learned to provide and refine a similar maritime tool.⁴

Grassroots Efforts

Furthermore, significant efforts within our nation's ports address local cybersecurity vulnerabilities. For example, in the Ports of Los Angeles/Long Beach, two local groups specifically address cybersecurity initiatives. Although not yet official subcommittees to the AMSC, each group has a direct linkage to the area maritime security committee via common membership.

The Los Angeles Port Police chairs the executive-level group, which consists of port security directors, police chiefs, the FBI assistant special agent in charge, the Secret Service supervisory special agent, and the Coast Guard captain of the port. This group focuses on high-level organizational

and policy changes, noteworthy national activity regarding cybersecurity, and port-wide projects, such as installing a fiber optic network to allow local Coast Guard sector personnel to monitor port police security cameras.

HOMEPORT and other information sharing protocols enable ports and area maritime security committees throughout the country to have access to the same information.



Cyber Threat Information Management

In August 2013, the U.S. Coast Guard released information stating that the official way to report cybersecurity incidents/breaches to the agency is via the National Response Center (NRC). This is wholly appropriate, as industry is already well familiar with the reporting protocol to the National Response Center.

Before then, cyber incident reporting had been rare. Between 2010 to 2013, fewer than five incidents were reported to the Coast Guard, since reporting has not been mandatory, unless the cyber incident leads to a transportation security incident.

Moreover, minimal reporting could be due to any of several factors, including lack of awareness that cyber incidents should be reported to NRC, lack of facilities actually monitoring the integrity of their cyber system security, failure of industry information technology personnel to communicate

breaches to the facility/vessel security officers, and/or lack of recognition of the risks inherent in cyber systems. Existing information sharing pathways throughout the Coast Guard and with port partners are largely appropriate for handling the sharing of cyber threat information, with a few modifications that are currently underway.

When NRC receives a cybersecurity incident report, it is immediately relayed to the proper Coast Guard sector and CG Cyber Command and then to the Intelligence Coordination Center. The sector may investigate and develop an intelligence report and transmit it to the Maritime Intelligence Fusion Center and/or the district intelligence office, and office personnel may issue an intelligence product to inform future operational decision making. Finally, the National Cybersecurity and Communications Integration Center, the DHS National Operations Center, and any

applicable local fusion center, as well as pertinent state and local agencies, may receive the incident report.

Coast Guard leaders recognize cybersecurity incidents must be treated with confidentiality, otherwise the maritime industry may be reluctant to report any security breaches. Depending on the nature of the breach, information contained in a report may identify significant vulnerabilities in a company's system or protocols. Therefore, procedures for sharing sensitive information among necessary parties must ensure that it is carefully controlled at all cognizant government offices, without unduly hindering sharing by adding a "secret" or higher classification.

Coast Guard personnel also post cybersecurity policy, threat information, and best practices on Homeport for industry partners with granted access.

A second group, which includes facility security officers and facility information technology personnel, Coast Guard information technology and port security specialists, and FBI and Secret Service agents, addresses cybersecurity's technical side. This group also has significant membership crossover with the official AMSC facility security officer subcommittee, enabling direct appropriate information flow from this group into the area maritime security committee, as a whole.

The Way Forward

The federal government cannot address MTS cybersecurity vulnerabilities and risks in a vacuum. We must continue outreach to all levels of government and industry, initiate discussions with port partners, and harness industry best practices to overcome cybersecurity threats. At the same time, Coast Guard leadership is refining internal priorities, intelligence collection processes, response protocols to cyber incidents, and information sharing procedures to ensure that cyber threat information reaches the correct parties for analysis and action.

About the author:

LCDR Maureen Johnson is a 2001 graduate of the U.S. Coast Guard Academy. A career prevention specialist, she has worked in facility and vessel inspections, port security, marine casualty and suspension and revocation investigations, aids to navigation, and waterways management. She has a master's degree in Leadership, Disaster Preparedness and Crisis Management from Grand Canyon University.

Endnotes:

1. Available at www.dhs.gov/national-infrastructure-protection-plan.
2. Captain of the Port authority is described in 33 CFR Subchapter P, the implementing regulations of the Ports and Waterways Safety Act, 33 USC 1221. As such, the COTP enforces regulations that protect vessel, harbor, and waterfront facility security, and holds authority, including over anchorages, security zones, safety zones, regulated navigation areas, ports, waterways and deepwater ports.
3. Federal maritime security coordinator is an additional title given to the captain of the port. It is not an entirely separate authority. With the title comes the authorization to establish and administer the AMSC and plan, as outlined in 33 CFR 103.205.
4. Energy Department Develops Tool with Industry to Help Utilities Strengthen Their Cybersecurity Capabilities. June 28, 2012. Available at <http://energy.gov/articles/energy-department-develops-tool-industry-help-utilities-strengthen-their-cybersecurity>.

Reach the National Response
Center at (800) 424-8802.

Countering the Maritime Cyber Threat

The FBI's expanding partnerships and programs.

by SUPERVISORY SPECIAL AGENT RICHARD KOLKO
FBI Cyber Division

Cyber crime is multifaceted and multi-jurisdictional, and effectively addressing this threat requires a new perspective on innovation and collaboration. Because of computer technology's constantly evolving nature and the fact that its misuse affects national security and all sectors of our economy and government, the FBI is evolving its tactics to include a fleet of fully engaged partners and deploying a host of learning programs and support capabilities to enable its cyber teams.

The FBI is dedicated to securing U.S. critical infrastructure from cyber threats in partnership with other government agencies and the private sector. FBI Director James Comey said, "The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas through cyber intrusions. That is why we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber-based terrorist threats."

Navigating the New Threat Horizon

Cyber threat actors pose the potential to disrupt critical infrastructure sectors, including transportation, under which maritime resides. To combat this array of new threats, we must first identify and try to understand them.

Our focus has revealed that cyber criminal groups commonly use computer intrusions to capture user names and passwords and extract companies' assets through illicit wire transfers. Further, nation-states are more concerned with using cyber tools for remote espionage, often siphoning documents from U.S. networks to overseas intelligence agencies. Moreover, of growing concern, cyber terrorists continually search for new and accessible methods to cause physical destruction from remote locations using computers. Hacktivists (users who hack or break into a computer system for a politically or socially motivated purpose), while typically considered less worrisome, can still cause tremendous damage, as they deface and use denial of service attacks to disrupt government and business websites.

While the FBI's assessment of cyber threats to the maritime realm remains low, each type of cyber threat actor has the potential to pose a considerable threat to the maritime sector.

For example, the maritime sector uses numerous industrial control systems to manage its port and shipping operations, and as these systems become increasingly networked and automated, the number of points cyber actors may exploit to disrupt the maritime sector will also increase. The FBI continues to monitor these cyber threat actors and their activity in the maritime sector.



GPS Spoofing

In the transportation context, GPS spoofing is the purposeful redirection of a vehicle to an unintended location through manipulation of the vehicle's GPS signals. Typically, this is achieved by sending signals to the vehicle's GPS receiver that are stronger than the signals coming from the legitimate GPS satellite source. This causes the vehicle to lock onto the false signals, and may allow a malicious actor to insert false data into the coordinates system.

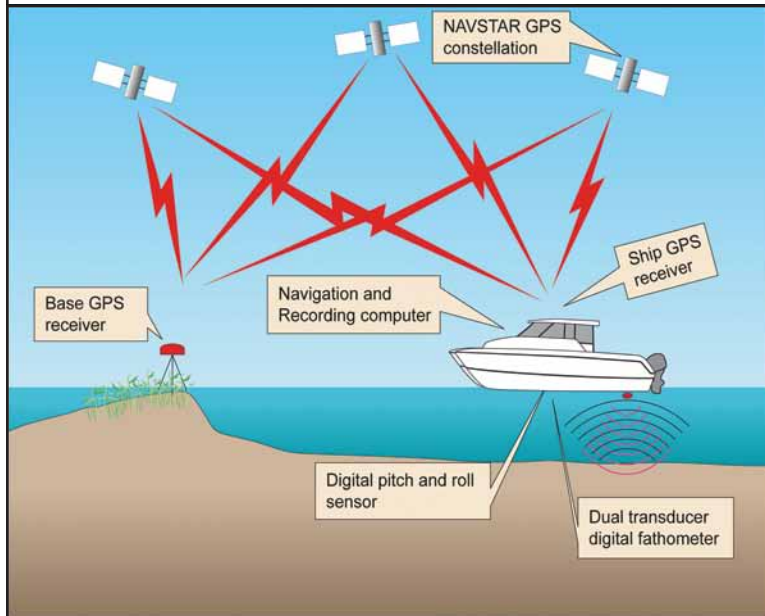


Image courtesy of US Geological Survey.

High Stakes on the High Seas

Beyond maritime ports, ships are vulnerable to remote cyber disruptions. It is theoretically possible to block or send false signals to a ship's Automatic Identification System, which could show vessels to be on an incorrect course or not in their actual position. Fraudulent signals could even show phantom ships.

The FBI, however, does not view these cyber threats as abstract or theoretical. In November 2013, the *Government Security News* published an article that outlined the \$1 billion a day in losses to the national economy that a cyber attack at a major port like Los Angeles or Long Beach could cost. The director of information at the Port of Long Beach noted that personnel block about 9 million network attacks each month.¹ But it only takes one successful intrusion to cause damage.

Somali pirates already have capitalized on this low level of cyber and information security. In 2011, pirates used easily available cyber tools to research the Internet for information regarding ships passing through nearby waterways.² They then scanned for communications signals onboard the ships to locate vessels transporting valuable cargo.

As the Somali pirates face increased naval pressure, the pirates have focused more on kidnapping Western crews and less on ransoming ships. However, they continue to do their research online. Pirates and their

Leading the Way Forward: The FBI's Legal Mandate

Presidential Policy Directive 21, which addresses critical infrastructure and resilience, provides one of several authorities the FBI operates under in the cyber arena. The directive's overarching goal is to strengthen the U.S. critical infrastructure security and resilience against physical and cyber threats.

Key elements of the mandate are to create added resilience at all levels and empower the public and private sectors to reinforce their own security through improved communication and connectivity with the federal government. The directive also gives the FBI specific authority to lead investigations and related law enforcement activities across the critical infrastructure sectors to address these threats.

The FBI also collects, analyzes, and disseminates domestic cyber threat information to interagency partners and the private sector. All of these efforts are closely coordinated with the Department of Homeland Security and other interagency partners.

foreign facilitators scour the Internet for available information about ships, cargos, tracks, and locations. In addition to piracy, threat actors around the world may use cyber tools to target the maritime industry for traditional theft and crime.

Cyberhood Watch

As part of a pilot project, FBI Los Angeles personnel developed an information sharing program with the ports in Los Angeles and Long Beach. The project, Cyberhood Watch, enables confidential, real-time cybersecurity and intrusion information sharing among members of the port “neighborhood” and the FBI. This helps cyber task force (CTF) agents and analysts to better understand the threats in the ports and allows them to build relationships with the public and private sectors.

In carefully examining potential disconnects and investigative gaps, agents identified a disparity in the ways federal, state, and local jurisdictions were addressing certain aspects of cyber crime. To address this, FBI personnel, in coordination with the Internet Crime Complaint Center, developed Operation Wellspring to pursue state and local prosecutions when federal prosecutorial guidelines could not be met.

Piloted in the Salt Lake City field office, the cyber task force agents worked closely with the U.S. Attorney’s office and the Salt Lake County District Attorney’s office to identify and develop cases for prosecution at the state and local level. More cities are being added to this successful, ongoing operation.



Online Training

Training our workforce on cutting-edge technology is essential, and cyber online training libraries are now offered to FBI personnel as well as to CTF federal, state, and local partners through Virtual Academy, Skillsoft, and Blackboard. The FBI is also developing a cyber investigator certification program engineered to educate federal, state, local, and tribal partners on cyber tools and investigative best practices.

This training will align with the White House-led National Initiative for Cybersecurity Education, which collaborates with more than 20 federal departments and agencies. The certification program will provide a sustainable workforce development solution consistent with national training and certification standards.

Partnership Programs

Another critical element to combat physical and cyber threats to the maritime sector is the Maritime Security



Pirates leave a merchant vessel for the Somali shore, while under U.S. naval observation. Photo by Petty Officer Jason Zalasky, courtesy of Navy Media Content Services.

Program (MSP) housed within the FBI’s National Joint Terrorism Task Force (NJTTF). NJTTF/MSP program managers work with field offices that have navigable waterways and ports by managing the Maritime Liaison Agent (MLA) program. These field office MLAs address terrorism and cyber threats directed against maritime assets and assist federal, state, and local agencies responsible for maritime security.

Due to the nature of these threats, MLAs now work more closely with their CTFs in each field office. Special Agent David Pileggi of the USCG Investigative Service is assigned to the FBI JTTF in Houston. He notes, “The MLA program pays dividends for maintaining maritime security. The partnership between the FBI and the Coast Guard allows real-time sharing of both operational information and intelligence and allows us to address maritime threats in a much more timely and efficient manner.”

A recent example of success with this program is the FBI San Francisco Field Office (SF) where the MLA and an intelligence analyst meet regularly with the Northern California Area Maritime Security Committee and the Multimodal Information Sharing Team. The USCG invited FBI SF to join the new cybersecurity subcommittee, and the Coast Guard Cyber Command invited the MLA to participate as a law enforcement partner on the USCG Homeport Web portal, which is a mechanism to share cyber-related threats and information and make it available to all maritime stakeholders. This partnership allows the FBI to serve as a force multiplier for the Coast Guard in the maritime security environment for physical and cyber threats.

Outreach and Partnership Information Sharing Programs

The FBI is actively sharing threat data with the private sector and partnering with DHS to transmit cyber threat

continued on page 60



The Unfolding Threat to Maritime Security

A Case Study



The Orange County Regional Computer Forensics Laboratory is part of a national network of FBI-sponsored, full-service forensics laboratories and training centers devoted entirely to the examination of digital evidence in support of federal, state, and local criminal and terrorism investigations. Photo courtesy of the Federal Bureau of Investigation.

A team of FBI agents from the cyber task force and Coast Guard Investigative Service meet in a warehouse on the outskirts of a major port on the West Coast to review the operations plan for a search warrant to be served on a nearby shipping office. The warrant is based on a cyber criminal intrusion into the office's computer system. The goal of the criminals in this scenario is to affect delivery of food shipments into the busiest port in the U.S. by hacking into the company's network, which can impact citizens through even a slight delivery delay.

Once the team leader finishes the standard entry and safety procedures brief, she introduces the bureau's Computer Analysis Response Team leader, who will determine how the computers, peripherals, and storage devices in the case will be seized.

The Partnership Solution

The FBI/Coast Guard team may conduct this type of maritime exercise scenario (which mimics the cyber threat that could emanate from literally any corner of the globe) at any time in the ongoing fight against cyber bad actors.

In preparation for an actual attack, an FBI-led, 19-agency team is standing by at the National Cyber Investigative Joint Task Force (NCIJTF). The task force itself teams with the operational sections of the FBI's Cyber Division to quickly analyze data from any seized items.

The FBI's Cyber Outreach team is also on standby. The Guardian Victim Analysis Unit, partnering with the FBI's cyber task forces in all 56 field offices are poised to notify potential victims of the intrusion. The National Infrastructure Protection Unit is prepared to notify its InfraGard membership of thousands about the vulnerability via a secure Web portal and by leveraging coordinators throughout field offices nationwide. Additionally, the Key Partnership Engagement Unit is ready to contact partners



FBI Portland SWAT team members drill aboard a ship as part of their maritime certification. Photo courtesy of the Federal Bureau of Investigation.

from the critical infrastructure sectors regarding the current threat and provide indicators their chief information security officers can utilize to identify the threat and counter the attack.

At the same time, the Cyber Initiative and Resource Fusion Unit team is standing by in Pittsburgh, Pennsylvania. The

The National Cyber Investigative Joint Task Force (NCIJTF) is the independent interagency cyber center that develops and shares information related to cyber threat investigations and coordinates and integrates associated operational activities to counter adversary-based cyber threats. The NCIJTF is an alliance of peer agencies with complementary missions to protect national cyber interests and the political, economic, and overall vitality of our nation.

Representatives from participating agencies and from federal, state, local, and international law enforcement partners have access to a unique, comprehensive view of the nation's cyber situation while working together in a collaborative environment, in which they maintain the authorities and operational/investigative responsibilities of their home agencies.

NCIJTF Members

Federal Bureau of Investigation



National Security Agency



Central Intelligence Agency



Department of Homeland Security



U.S. Cyber Command



U.S. Secret Service



Defense Security Service



Air Force Office of Special Investigations



Department of State Office of Computer Security



G2X Cyber CI, 902nd Army Research Lab



Defense Criminal Investigative Service



Naval Criminal Investigative Service



Cyber Crime Center Analytical Group



Defense Intelligence Agency



DOE Office of Intelligence and Counterintelligence



National Geospatial Intelligence Agency



National Reconnaissance Office



Department of Justice



National Aeronautics and Space Administration



fusion unit is positioned with the National Cyber Forensic and Training Alliance (NCFTA) and participates in the NCFTA's international model for synching law enforcement, private industry, and academia to share information to mitigate or stop emerging cyber threats.

FBI Los Angeles Assistant Special Agent in Charge Gina Osborn is well versed in the potential harm cyber actors can inflict in the maritime environment. She said, "We plan these types of exercises in coordination with our partners in anticipation of the growing cyber threat. It sounds like a cliché, but it really is one of those scenarios where we are aware that it's

a matter of *when*, not *if*. Preparation and training are key to our success."

The FBI Cyber Division's Assistant Director Joseph Demarest explains, "This situation may only be a drill, but this type of intrusion can occur anytime and emanate from anywhere. The FBI's Cyber Division, in conjunction with the NCIJTF, is in place to work with the intelligence community, and federal, state, and local law enforcement, as well as our international partners, in the event of a cyber emergency. There is a lot going on here at the NCIJTF and at headquarters, but our cyber task forces in the field are the true tip of the spear."

Building Agility to Outpace Cyber Adversaries

The FBI launched the Cyber Division in 2003, which has since continued to grow and adapt to an ever-evolving threat. The FBI, in fact, elevated the cyber threat to its number-three national priority, after counterterrorism and counterintelligence. With this type of growth comes the need for specially trained personnel, and the bureau is hiring technically trained agents, analysts, computer scientists, and forensic specialists. Through its liaisons with law enforcement, private industry, and academia, and through initiatives like the Domestic Security Advisory Council, InfraGard,¹ and the National Cyber Investigative Joint Task Force, the FBI is making partnerships and training a top priority.

With the bureau's cyber threat operational tempo increasing at warp speed, the need for immediate awareness and information sharing necessitated standing up a 24/7 cyber operations center. Cyber Watch now serves as the FBI cyber program's operations center for intrusion response operations and provides immediate connectivity to U.S. government cyber centers and FBI

legal attachés (LEGATS) stationed around the world, as well as our public and private sector partners.

When an event requires response, the FBI maintains cyber action teams that can be deployed around the world on a moment's notice to assist in computer intrusion cases and gather vital intelligence that help identify the cyber crimes that are most dangerous to our national security and to our economy. Our cyber-specific LEGAT program also is rapidly growing, with agents now stationed in numerous embassies overseas to liaise with law enforcement partners. Moving assets closer to the problem helps speed information flow and facilitate information sharing to deter rapidly developing cyber threats.

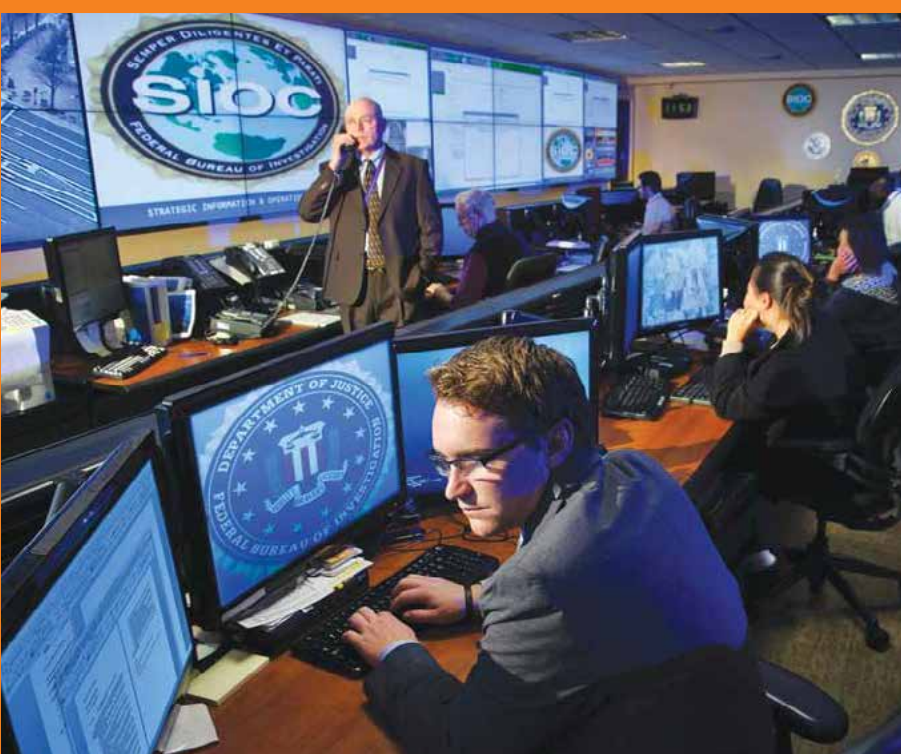
Endnote:

¹ InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S. See <https://www.infragard.org/>.

Identify, Pursue, Defeat

“Our Cyber Division motto is, Identify/Pursue/Defeat, and as we continue to engage threats in the cyber arena, it will be our ability to adapt, train, prepare, share, and respond effectively that will keep our nation, our economy, and our citizens safe.”

—FBI Cyber Division Assistant Director Joseph Demarest



information to state, local, tribal, and territorial authorities. While engagement with all critical infrastructure sectors is actively taking place, the FBI's Cyber Division focuses first on those sectors deemed most critical to our national security—energy, finance, technology, telecommunications, healthcare, and transportation (including maritime).

Several entities within the FBI operate these strategic-level information sharing partnerships. InfraGard, a partnership between the FBI and the private sector, and the cyber task force agents remain at the forefront of the outreach programs in each field office for cyber matters. At FBI headquarters, several units, not only in the Cyber Division, but throughout headquarters, conduct critical liaison and outreach to build

The Strategic Information and Operations Center at FBI headquarters is the 24/7 command post that monitors FBI operations and law enforcement activities around the globe. Photo courtesy of the Federal Bureau of Investigation.

trust, develop effective working relationships, and drive timely information sharing.

Information sharing methods with industry partners include private industry notifications (PINs) and FBI liaison alert system reports. For example, a maritime-specific PIN, “Maritime Supply Chain Vulnerable to Cargo Theft,” recently highlighted a serious cyber vulnerability to the maritime industry.³

The FBI remains determined to develop and deploy creative solutions to defeat today’s complex cyber threat actors. Instead of reacting to cyber threats, we must also build better relationships, overcome the obstacles that prevent us from sharing information and, most importantly, continue to step forward to collaborate with partners across government and the private sector.

About the author:

Special Agent Richard Kolko joined the FBI in 1996 and is currently assigned to the Cyber Division. He has served in Atlanta, New York, and at headquarters, and has conducted investigations on five continents. Special Agent Kolko served on the Joint Terrorism Task Force, deployed to Iraq, was chief of the National Press Office, and a National Academy instructor. He served in the Navy as a P-3 pilot and reserve intelligence officer, retiring as a commander in 2011. He has a bachelor’s degree in communication from the University of Miami, and a master’s degree in homeland security from American Military University.

Endnotes:

1. Available at www.gsnmagazine.com/article/39138/cyber_attack_major_port_could_cost_1_billion_day.
2. Available at www.nationaldefensemagazine.org/archive/2012/May/Pages/PiratesExploitingCybersecurityWeaknessesinMaritimeIndustry.aspx.
3. Maritime Supply Chain Vulnerable to Cargo Theft, March 26, 2014. Available at https://www.osac.gov/Pages/ResourceLibrary.aspx?CategoryId=7&ctl00_ctl14_g_b21907d9_dde3_4c37_8858_3b9dd657f773_ctl00_linksRadGridChangePage=12&ctl00_SPWebPartManager1_g_b21907d9_dde3_4c37_8858_3b9dd657f773_ctl00_linksRadGridChangePage=5_20.

Bibliography:

- Anderson, T. Cyber-attack at a Major Port Could Cost \$1 Billion per Day. *Government Security News*. N.p., 24 November 2013. Web, May 9, 2014. Available at www.gsnmagazine.com/article/39138/cyber_attack_major_port_could_cost_1_billion_day.
- Bryant, D. L. Marine Cybersecurity: Is Your Ship Safe? Are You. *Marine Link*. Maritime Reporter & Engineering News, Jan. 2, 2014. Web, May 9, 2014. Available at www.marinelink.com/news/cybersecurity-marine-your362503.aspx.
- Demarest, J. Personal interview Apr. 24, 2014.
- European Union Agency for Network and Information Security. *Cyber Security Aspects in the Maritime Sector* — ENISA. N.p., Dec. 19, 2011. Web, May 9, 2014. Available at www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts.
- Farivar, C. Professor Fools \$80M Superyacht’s GPS Receiver on the High Seas. *Ars Technica*. Conde Nast, 29 July 2013. Web, May 9, 2014. Available at www.arstechnica.com/security/2013/07/professor-spoofs-80m-superyachts-gps-receiver-on-the-high-seas.
- Frod, M. G. “Pirates Exploiting Cybersecurity Weaknesses in Maritime Industry.” *National Defense*. National Defense Industrial Association, May 2012. Web, May 9, 2014. Available at www.nationaldefensemagazine.org/archive/2012/May/Pages/PiratesExploitingCybersecurityWeaknessesinMaritimeIndustry.aspx.



An FBI SWAT operator boards a cargo ship during an annual maritime training exercise, designed to hone FBI SWAT team members’ abilities in the event of a terrorist attack, hostage situation, or criminal or national security threat. Photo courtesy of the Federal Bureau of Investigation.

Honoroff, M. “Cops Shut Down Hacker Drug Ring.” *Msnbc.com*. June 19, 2013. Web, May 12, 2014. Available at www.nbcnews.com/id/52242128/ns/technology_and-science-tech_and_gadgets/t/cops-shut-down-hacker-drug-ring/.

Osborn, Gina. Personal interview. April 10, 2014.

Presidential Policy Directive – Critical Infrastructure Security and Resilience. The White House. The White House, Feb. 12, 2013. Web, May 9, 2014. Available at www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Statement before the Senate Committee on Homeland Security and Governmental Affairs (2013) (testimony of James B. Comey, Director Federal Bureau of Investigation). Web. Available at www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response.

Vargas, J. *Drug Cartels Hacking Shipping Companies — Seaports Are Targets*. InterPort Police. June 18, 2013. Intelligence Briefing compiled by the InterPort Police Law Enforcement and Public Safety Research Services Center.

Rethinking Reporting

Handling transportation cybersecurity incidents.

by MR. WESTON R. LAABS
Intelligence Operations Specialist
U.S. Coast Guard, Sector Lake Michigan



A Vessel Traffic Service workstation displays various means used to monitor maritime traffic including Coast Guard Vessel Traffic System, Automatic Identification System, radar and closed-circuit television. U.S. Coast Guard photo by Petty Officer Nathan Bradshaw.

Highly publicized examples of cyber breaches in the marine sector, such as successful hacking of the Automatic Identification System (AIS),¹ have shed light on the cybersecurity challenges that the maritime industry must face and work toward securing.

Today, cyber breaches have garnered so much attention in the security world that government organizations, think tank researchers, academia, and the private sector are all clamoring to develop best practices, recommendations, and regulations to help fit the emerging challenges.

Cyber Security and the Marine Transportation System

For decision makers and planners, understanding the complexities, uncertainties, and dynamic nature of the cyber domain is critical for understanding vulnerabilities and threats, developing appropriate courses of action, and evaluating metrics and measures of effectiveness. As enterprises and organizations rely more wholly on computer networks for operations, data storage, and communications, they will become increasingly desirable targets for identity thieves, hackers,² state actors, and extremists.

Perhaps one of the most pressing aspects of increasing cybersecurity awareness is that personnel in positions best situated for mitigation and response do not always know enough. For example, the U.S. Coast Guard intelligence specialists to an area maritime security committee (AMSC) provided a maritime cyber threat intelligence briefing not too long ago. During the question-and-answer session, one AMSC executive steering committee member announced that their server computers are kept at night behind a locked

door. "So, we're good," when it comes to cyber security. Some information assurance and technology professionals may be floored by such a statement, but this is the reality of it.

The media continues to report daily information about security breaches, leaving millions of credit cards, health records, or other personally identifiable information in criminal hands. Most people are fully aware of the impact that cyber breaches can have on business payroll accounts and operational environments within critical infrastructure sites; however, facilities continue to report to the National Response Center (NRC) a tourist taking photographs of a critical infrastructure facility's smoke stack, because he thought it looked cool. It's 2014, and the mindset needs to change.

Implementing Cyber-Specific Security Plans

The U.S. Coast Guard's authorities and missions have long revolved around search and rescue, defense, homeland

Developing Post-Incident Response and Recovery Plans

Two major inhibitors prevent incident reporting:

- perceived lack of governmental ability to respond and assist with such an attack,
- lack of cyber-specific incident response plans.

Well-established security and response plans exist from all levels of government and the private sector to respond to, mitigate, and recover from all types of physical security breaches and attack scenarios, yet many organizations do not know who to contact when a cyber intrusion is detected or have plans in place that quantify cyber-specific breaches.

Similarly, while many government agencies are prepared for physical security response, they may not have the capabilities or expertise to assist in recovery from a cyber incident. For example, would the Coast Guard marine security technicians that regulate MTSA facilities and normally respond to physical security breaches have the knowledge, skills, and abilities to assist IT staff at an affected organization?

As agencies build exercise plans, cyber should be stressed as an essential element, specifically as the method behind the root problem of the scenario. Bringing cyber to the forefront of exercise planning, preparation, and execution is critical to explore the problem and its response, prior to an actual incident.

security, and maritime law enforcement. The Maritime Transportation Security Act (MTSA) of 2002 requires vessels and port facilities to develop security plans and conduct vulnerability assessments. The USCG regulates these screening plans, which involve screening procedures, establishing restricted areas, personnel identification procedures, access control measures, and site surveillance equipment.

Currently, there is no requirement mandating cyber-specific security plans or vulnerability assessments. However, MTSA-regulated vessels and facilities are required to report security incidents that meet the threshold of a transportation security incident (TSI)—any incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruption to a particular area.³ In the Great Lakes, the lion's share of transportation security incidents involve small-quantity oil spills and/or discharges and security breaches to critical infrastructure facilities.

Due to increased awareness of the “See Something, Say Something” public awareness campaign, many facilities report pre-incident indicators of terrorism to the National Response Center—events such as suspicious photography or surveillance of critical infrastructure sites, eliciting

Additionally, exercise planners are required to consider expanding exercises to include organizations and personnel not normally affiliated with maritime security. This move will greatly enhance the content shared at the exercise and bring legitimacy through subject matter expertise in response and recovery capability scenarios.

One of the main issues with exercise planning in its current form is the unnecessary isolation of cyber elements when planning exercises. The cyber and physical worlds are intertwined, and exercise scenarios must be written to accommodate both environments. What planners and exercise participants should understand is that there is not a need to inundate players with technical details about cyber attacks. Many cyber-specific scenarios begin with an electronic malfunction; however, cyber elements almost always bleed into the physical environment, requiring first responder intervention and other typical disaster recovery decisions.

For example, a cyber attack at a MTSA-regulated chemical facility causes a hazardous spill. Of course, there is a physical response: local police and fire, emergency management personnel, and federal agencies, if necessary. So it makes sense to integrate cyber-specific exercise scenarios into other response exercises.

information about access control or security, or physical security breaches such as theft from within a secured area. Although these types of incidents meet the threshold required for “suspicious activity,” there is currently no regulation or requirement to report any cyber-specific incidents. However, the Coast Guard and the Department of Homeland Security are making inroads to tackle this issue.

Training the Right Person for the Position

While it is possible to organize an institutional change when addressing an issue as complex and far-reaching as cybersecurity, a complete overhaul of personnel across the maritime environment to address cyber security insufficiencies is simply not operationally feasible, or the best option in many situations. Training existing personnel in cyber security issues, while also refocusing efforts from physical security and toward cyber, may be a viable alternative. Personnel already in these positions may have knowledge, skills, and expertise unique to their posts that cannot always be matched or filled by cybersecurity experts.

Additionally, the foray into cyber incident reporting best practices should begin by limiting the requirements to only those events that involve physical as well as cyber infrastructure. The best way to explain “cyber” without

immediately causing the audience to tune out is to relay cyber as a method, not a target.

Cyber incident reporting needs to be secured and handled separately than other suspicious activity reports. The Department of Homeland Security has time-tested abilities to receive and report on cyber-specific incidents without compromising public trust of the reporting organization. Actionable intelligence is not derived from the name of a victim; instead, the bad actor's tactics, techniques, and procedures are the real substance of any report. Specific attacking IP addresses, intrusion methods, and malware filenames, and hashes are extremely useful to organizations trying to secure systems from attack. Assuring timely actionable technical information reporting related to cyber attacks will offer cross-sector personnel the best chance to mitigate the same or similar attacks against their own network infrastructures.

Embracing Changes

Cyber crime is not going away. In the homeland security and emergency management worlds, there are constant responses to new threats and challenges, including radiation detection equipment, anthrax awareness, and active shooter training. All have been recently promoted as necessities to improve resilience among first responder communities. However, unlike these evolving threats and challenges, cybersecurity is deeply interwoven into almost all aspects of life. From our basic utilities to our communications platforms, all are dependent upon functioning cyber platforms.

As cyber continues to grow in importance, investing in its security is the best chance we have to remain one step ahead of the criminals and hacktivists attempting to uproot the system. Therefore, to keep up with emerging cyber technology and threats, constant interaction between the public and private sectors is critical, but cannot remain as one-sided as it has in the past. MTSA-regulated and other critical infrastructure facilities will only report cyber breaches to the

NRC if these organizations receive some tangible benefit from reporting. It is the duty of the public sector, including elements at all levels of government, to establish response plans to cyber incidents so recovery plans are in place. Successful mitigation and recovery will lead to future reporting, which better arms the government with information about attacks. This reporting and recovery cycle continues to feed itself, creating the best scenario for the most up-to-date threat information, combined with the best possible tools to respond to such threats.

Although it remains perceptibly different from physical security in the eyes of many in the emergency preparedness communities, cybersecurity follows all the same requirements when it comes to recovery. Instead of framing cyber as its own problem with its own solutions, it is necessary for local communities to address the issue head-on and comprehensively, knowing that cyber insecurities can create physical problems. Without preparing for the future effectively, we will simply be unsuccessful when it comes to recovery.

About the author:

Mr. Weston R. Laabs is an intelligence operations specialist at U.S. Coast Guard Sector Lake Michigan. In this capacity, he functions as the sector intelligence staff cybersecurity specialist. Prior to this position, he served as an intelligence analyst with the Michigan Intelligence Operations Center, Michigan's DHS-sponsored fusion center. He holds a master's degree in law enforcement intelligence and analysis and a bachelor's degree in international relations from Michigan State University.

Endnotes:

- ¹ Visit www.computerworld.com/article/2475227/cybercrime-hacking/hack-in-the-box--researchers-attack-ship-tracking-systems-for-fun-and-profit.html.
- ² A hacktivist is a computer hacker whose activity is aimed at promoting a social or political cause.
- ³ See www.uscg.mil/d8/msuBatonRouge/mtsa.asp.

Bibliography:

Cyber Security and the Marine Transportation System (MTS). ALCOAST 122/14. Washington, DC: U.S. Coast Guard, 2014. Available at www.uscg.mil/announcements/alcoast/122-14_ALCOAST.txt.

The Maritime Transportation Security Act of 2002.

Available at www.gpo.gov/fdsys/pkg/PLAW-107publ295/pdf/PLAW-107publ295.pdf.

Cyber Intelligence Operations

More than just ones and zeroes.

by RANDY BORUM, PH.D.

*Professor and Coordinator for Strategy and Intelligence Studies
School of Information
University of South Florida*

JOHN FELKER, CAPTAIN USCG (RET.)
*Director, Cyber Intelligence Strategy
HP Enterprise Services*

LIEUTENANT COLONEL SEAN KERN, USAF
Joint Forces Staff College Joint Advanced Warfighting School

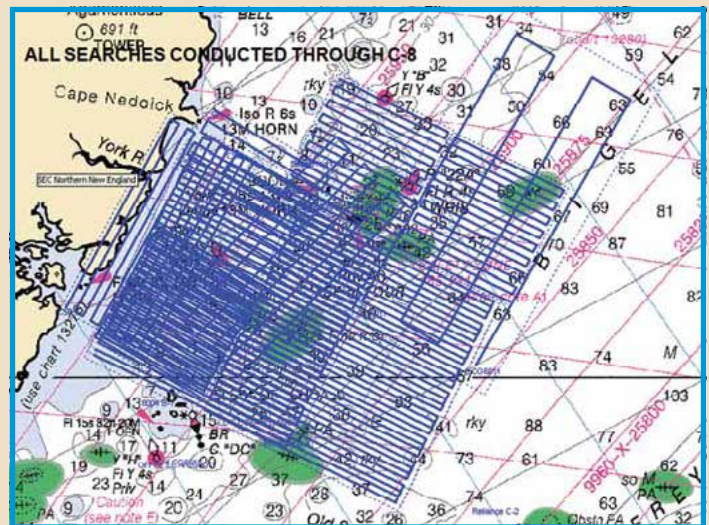
Today's Coast Guard relies heavily on digital information and communication technologies. In fact, every aspect of Coast Guard operations and support relies upon network resources for function, sorting, analysis, storage, and communication.

For example:

- Rescue 21, the Coast Guard's short range communications, direction-finding tool is completely digital and connected to the Internet.
- National security cutters integrate engineering, weapons, communications, and intelligence and administration systems electronically and are connected to the Internet.
- Computer-driven acquisitions, stores, and replacement management powers logistics management service-wide, connected to the Internet.
- Regulated maritime critical infrastructure uses computers for cargo management and movement as well as physical security. These systems are Internet facing, if not connected.

In short, the Coast Guard and infrastructure operators rely on digital information and communication technologies. Because these systems are Internet-facing, the Coast Guard, like other government agencies and commercial enterprises, is threatened by malicious actors seeking to disrupt operations, steal information, and

cause other bad things to happen in the cyber domain. Moreover, Internet-facing systems provide an attack surface through which these cyber threat actors can gain access to achieve their objectives.



A computer-generated image of a Coast Guard search pattern chart. Increasingly, search planners rely on computer-generated search planning and Rescue 21 communications, direction-finding, asset tracking, and case file management. If these systems are obstructed or the data altered through a cyber intrusion, there is considerable chance that not only will operational effectiveness be compromised, but lives may be lost. U.S. Coast Guard photo.

What is Cyber Intelligence?

Cyber threats are often regarded as technical challenges. It is easy to forget that there are people behind the keyboards. Individual actors and groups have intentions, motivations, objectives, knowledge, and capabilities. They engage in a

range of behaviors while they are contemplating, planning, preparing, and executing an intrusion or attack in the cyber domain, the same way criminal organizations prepare for an illegal migrant or drug smuggling operation.



A marine science technician at Coast Guard Sector Baltimore and a Customs and Border Protection officer stand by while a container is inspected with a vehicle and cargo inspection system (VCIS), a tool used for non-intrusive container inspections. The VCIS takes X-ray images of containers to find illegal cargo, such as narcotics. It can be interfered with via cyber means if overall systems are not properly defended. U.S. Coast Guard photo by Petty Officer Robert Brazzell.

If understanding cyberspace is the goal, then a critical first step is to get ahead of the hack.

The Coast Guard must get a clear picture of its adversaries' capabilities, motivations, intentions, and activities in the cyber domain, before an attack, so personnel can develop proper operational countermeasures.

Additionally, understanding that actionable intelligence comes from knowledge, not just from a collection of data points, is a good first step toward scoping what comprises cyber intelligence. However, there are key points that must be established if the Coast Guard, or any enterprise for that matter, intends to fully implement a cyber intelligence-driven approach to cyber defense:

- The quest for relevant knowledge must look beyond the network. Technical collection is important, but it is not sufficient to counter the complex and evolving array of today's cyber threat actors.

According to USCG Publication 2-0, the purpose of intelligence is to inform commanders and decision makers by providing accurate, timely, and relevant knowledge about adversaries, threats, and the surrounding environment. In the Coast Guard, this surrounding environment includes the maritime domain and the cyber domain. Many Coast Guard members often narrowly interpret this as providing tactically actionable intelligence to operational forces and, as a result, measure the effectiveness of intelligence support accordingly.

- The cycle of collection, analysis, dissemination, and feedback must be a continuous—not a periodic or intermittent—process. The cyber domain is highly dynamic, so an effective defense posture must be agile and adaptive.
- Actionable cyber intelligence needs to inform all levels of operation. It must support decisions and decision makers at the strategic, operational, and tactical levels.

The Elements of Cyber Intelligence

Cyber intelligence should not only drive the Coast Guard's cybersecurity and cyber defense missions, it should be an enabling function for Coast Guard missions across the board. The scope of that intelligence must operate at strategic, operational, and tactical levels. This means

going beyond the network. Just as operational plans are routinely supported by intelligence from human and signals sources, an effective cyber defense plan must be similarly supported to anticipate and respond to specific threats, such as who is likely to attack, where, when, how, and why. Preparation for cyber defense operations and field operations involves assessing the adversary and the environment.

Just as Coast Guard operators evaluate the operational environment for a law enforcement operation, a marine facilities security inspection, or a search and rescue mission, so must they also consider its cyber operating environment within the context of a planned and dynamic defense, informed by cyber intelligence. Not only will cyber intelligence directly support operations in the field, it must also address actual threats and preparations for potential threats that engage in and through cyberspace. Firewalls and network logs are not sufficient. More proactive defense measures, informed by cyber intelligence, must be the way the Coast Guard protects itself and achieves a high level of mission assurance.

Reliance upon electronic means for operational planning and communications continues to grow, and maritime interests regulated by the Coast Guard increasingly rely on cyberspace and information and communication technologies to conduct essential mission and business functions. Therefore, understanding and effectively operating in that cyberspace environment is critical to mission success.

In developing its cyber strategy, the Coast Guard has a remarkable opportunity to lead America's homeland defense enterprise by developing a cyber intelligence-driven approach to cyber defense that corresponds with Coast Guard operations. A cyber intelligence-driven model has three distinct advantages, it:

- transforms the cyber defense posture from reactive to proactive;
- permits a shift from perimeter defense to maneuver operations;
- enables an adaptive cyber defense solution, based on a continuous assessment of cyberspace risk and its implications for the mission.

Beyond the Network

Cybersecurity professionals often do not think about intelligence in a comprehensive way. In fact, when addressing threat intelligence, many professionals focus only on technical/logical aspects. Though this information is useful, the main value of after-the-fact insights into an attack lies in their utility in preventing future, similar, attacks.

Tactical cyber intelligence, although necessary, is not sufficient to manage cyber risk. Cyber threats originate with people who are making decisions and acting within a context or environment to achieve certain objectives. Intelligence collection, therefore, should consider a range of adversary behavior and activity as well as geopolitical, social, industrial, economic, and cultural context. This provides a more comprehensive view of the attack surface and allows organizations to better anticipate and prevent attacks and malicious activity, not just respond to them.

Instead of thinking about cyber attacks as events, it might be more useful to consider them as a process, or the end result of a planning and preparation process. That approach implies a need to assess and understand potential adversaries, maintain situational awareness, and consider how the operating environment and features of our own organization or system might affect an adversary's actions and objectives.

Continuous Assessment and Adaptive Mitigation

Traditional cybersecurity approaches are static; they rely on filters, firewalls, and other perimeter defenses. Static methods can help defend against known threats, but they are ineffective against new threats and zero-day exploits. They are also insensitive to attack plans, preparations, and pre-incident indicators and warnings. Cyber threats move at network speed, after they have been weaponized and bad actors decide to attack. The only way to gain advantage is by using a continuous cyber intelligence process to anticipate potential threats and take preventive action.

Current cyber defense approaches are reactive and only adapt periodically. That posture will result in limited



A shipping container was dropped while being off-loaded at a container terminal. Supervisory control and data acquisition systems that are interconnected with port business systems can be hacked, causing malfunctions such as placing containers in the wrong spot or dropping them completely. Photo by Colin K. Work @ Pixstel.

success. There is a need to fundamentally change how the Coast Guard understands and operates in cyberspace. Personnel must perform active and ongoing assessments to create dynamic defenses and collect, process, and disseminate actionable cyber intelligence to support decisions and decision makers at the strategic, operational, and tactical levels of planning and execution.

Each of these levels of intelligence supports a different segment leader in an operation or business:

- At the strategic level of planning and execution, the focus is on establishing an organization's mission and direction, setting objectives, and developing a plan for how those objectives will be achieved. Solid strategic-level cyber intelligence can help focus the leadership on potential long-term cyber threat actors and vectors and thereby lead to more informed planning and resource allocation.



A petty officer tracks a Coast Guard cutter's position on a nautical chart. Navigation systems are critical to operations. Hacking or jamming these systems could significantly hamper effective operations. U.S. Coast Guard photo by Petty Officer Lauren Jorgensen.



Aids to navigation placement has become highly dependent upon electronic navigation and management systems that are vulnerable to hacking. U.S. Coast Guard photo by Petty Officer Ayla Kelley.

- At the operational level, the focus is on enabling and sustaining an organization's day-to-day operations and output, including logistics. The decision makers are managers who plan and implement network operations and defense, based upon the strategic resourcing guidance. So operational cyber intelligence informs planning efforts that make for more effective resource positioning and policy development.
- At the tactical level, the focus is on the specific steps and actions taken to enact a strategic operations plan. This is where cyber threat actors and network defenders maneuver against each other. Tactical decisions and activity focus on day-to-day, on-the-network operations and defense. These are often executed in the network operations or security operations center and may include security system alerts and signature or behavior-detection efforts.

In today's environment, cybersecurity requires a proactive, dynamic defense posture. Cyber intelligence is the foundation for this type of defense. Effective cyber defense plans are based on continuous internal and external assessments. Internally, an organization should assess and prioritize its assets and analyze key risks, vulnerabilities, and exposure. Externally, it should continuously assess and characterize its adversaries and competitors (including their intentions, objectives, methodologies, opportunities) and maintain high operating environment situational awareness.

Cyber intelligence can be leveraged to reduce uncertainty for decision makers and to prevent surprise events such as

disruptions or attacks. Cyber defense decisions are not just made in the network operations center, but throughout the organization. The challenge now is to enable all decision makers to fully understand what information is needed and how to work with a cyber intelligence service or team to collect it, integrate it, and make it accessible and actionable to those who must act on it to deter, thwart, or limit malicious network activity. By operating this way, the Coast Guard can successfully complete its wide array of missions and be assured that its systems are protected from cyber threat actors or, at a minimum, have procedures in place that facilitate continuity of operations through a cyber intrusion.

About the authors:

Randy Borum, Ph.D., is a professor and coordinator for strategy and intelligence studies in the School of Information at the University of South Florida. He previously served on the DNI's Intelligence Science Board (ISB), and has studied behavioral dynamics in violent extremism and counterintelligence. He has authored/co-authored more than 150 professional publications and currently serves as senior editor for the Journal of Strategic Security.

Capt. John Felker is director of cyber intelligence strategy at Hewlett-Packard Enterprise Services. His primary focus is developing business strategies for the Department of Homeland Security, Department of Defense, and the intelligence community. In his 30-year Coast Guard career, he commanded several vessels, served as a program analyst, led the Coast Guard's international training team, and stood up the Coast Guard Cryptologic Group as the first commander, and Coast Guard Cyber Command, as the first deputy commander.

Lieutenant Colonel Sean Kern is on the faculty at the National Defense University's Information Resources Management College, where he teaches cybersecurity, national intelligence, cyber policy, and terrorist and criminal use of cyberspace. He has commanded a space ground relay station and an expeditionary communications squadron, served at various organizational levels and deployed in support of Operation Iraqi Freedom and Operation Enduring Freedom.

Bibliography:

Dennesen, Kristen, Felker, John, Feyes, Tonya, and Kern, Sean. *Strategic Cyber Intelligence*. Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2014.

Bamford, George, John Felker, and Troy Mattern. *Operational Levels of Cyber Intelligence*. Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2013.

Ludwick, Melissa, Jay McAllister, Andrew D. Mellinger, Kathryn Ambrose Sereno, and Troy Townsend. "Cyber Intelligence Tradecraft Project: Summary of Key Findings." Software Engineering Institute, Carnegie Mellon University, 2013. Web. www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf.

Coast Guard Publication 2-0(CG Pub 2-0), Intelligence. Available at: www.uscg.mil/doctrine/CGPub/CG_Pub_2_0.pdf.

Named after co-founders Ron Rivest, Adi Shamir and Len Adleman.

RSA. *Getting Ahead of Advanced Threats*. Jan. 2012. Web. www.emc.com/collateral/industry-overview/ciso-rpt-2.pdf.

Combating Insider Threat

The greatest threats are the ones with access.

by MR. GREG SMITH
*Intelligence Specialist Chief
 Intel Division Senior Watch Officer
 U.S. Coast Guard Cyber Command*

The Scoop on Insider Threats

External cyber crimes and attacks are committed at an increasingly alarming rate, but can usually be mitigated by controlling access to data and detecting unauthorized access. However, threats that include sabotage, theft, espionage, and fraud continue to originate from within organizations, carried out through abusing access or mishandling physical devices to steal information. The cost of damage caused by insiders is unknown, as most crimes go unreported or undetected.

Most “inside jobs” happen because employers did not appropriately assess the risks and plan accordingly. The good news is that when appropriate insider threat-detection and prevention countermeasures are in place, the threat can be reduced dramatically.

The insider threat has matured, due to technology’s progression and now applies to information data systems. Although government and private industries identified the insider threat to information data systems years ago, mitigation strategies, until recently, have relied on nontechnical measures such as employee awareness and education, background investigations, and trust management.

In most cases, when insiders set out to harm an employer, they come armed with the trust and authority necessary to perform the malicious activity. While it is typical that normal access credentials are sufficient, some insiders go further and use conventional hacking methods, including password hacking, vulnerability exploitation, changing system configurations, and using login credentials stolen from coworkers. Copying or uploading proprietary data, either on the way out of the door to another job or sending to an outside party for direct financial compensation, is the most common crime.



Gen. Douglas MacArthur,
 Jan. 9, 1943. Photo courtesy
 of the U.S. Army.

“I am concerned for the security of our great nation; not so much because of any threat from without, but because of the insidious forces working from within.”

—General Douglas MacArthur

Insiders can profit and exact revenge in one fell swoop by selling valuable data and source code to an employer’s competitors. Or, in the age of zero-capital start ups, they can use customer lists to go into business for themselves. On the IT side, threats can sometimes take a bizarre turn, such as an individual refusing to give up passwords or other essential information. Some technically savvy insiders even go as far as installing a “time bomb” program to activate if the employee is laid off or fired.

Predicting which insiders may pose a threat can be an arduous task. While many malicious insiders are disgruntled and give prior warning of the damage they can accomplish, just as many are well-liked and trusted workers who give no indication of impending betrayal. No single personality model indicates who is more likely to pursue insider crime.

Recognizing the Signs of an Insider Threat

So it’s important to look for tell-tale actions or tendencies that may indicate a potential insider threat. Indicators include:

- **Greed or financial need:** A belief that money can fix anything. Excessive debt or overwhelming expenses.
- **Anger/revenge:** Disgruntlement to the point of wanting to retaliate against the organization.

Defining Insider Threat

An insider threat is a current or former employee, contractor, or business partner who:

- has or had authorized access to an organization's network, system, or data;
- can bypass existing physical and electronic security measures through legitimate measures.

—Software Engineering Institute, Carnegie Mellon, 2012.

- **Problems at work:** A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.
- **Ideology/identification:** A desire to help the “under-dog” or a particular cause.
- **Divided loyalty:** Allegiance to another person or company, or to a country besides the United States.
- **Adventure/thrill:** Want to add excitement to their life, intrigued by the clandestine activity, “James Bond Wannabe.”
- **Vulnerability to blackmail:** Extra-marital affairs, gambling, or fraud.
- **Ego/self-image:** An “above the rules” attitude or desire to repair wounds to self-esteem.
- **Vulnerability to flattery or the promise of a better job:** Often coupled with anger/revenge or adventure/thrill.
- **Ingratiation:** A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.
- **Compulsive and destructive behavior:** Drug or alcohol abuse or other addictive behaviors.
- **Family problems:** Marital conflicts or separation from loved ones.

Insider Threat Prevalence

Estimates of how often companies face attacks from within are difficult to make. In general, insider attacks are under-reported to law enforcement, prosecutors, and the media in general. Reasons for such under-reporting include an insufficient level of damage to warrant prosecution, a lack of evidence to prosecute, and concerns about negative publicity.

“If ignorant both of your enemy and yourself, you are certain to be in peril.”—Sun Tzu

While preventing all insider crime is impossible, employees and management need to understand that insider crimes do

occur and that they have severe consequences. In addition, it is important to understand that malicious insiders do not fit a particular profile. The technical abilities range from minimal to advanced, and the ages range from late teens to retirement age. There is no easy way to use demographic information to identify a potential insider threat. However, there are ways to identify higher-risk employees and implement mitigation strategies to reduce damage, should they choose to attack.

Insider Threat Best Practices

Best practices for preventing and mitigating insider threats are largely policy-centric. In many cases, these practices are the only realistic way to deal with insider threat problems.

“For most organizations, insider threats have moved beyond risk into reality; however, many threat vectors can be protected against with a measured approach to business security.”—Amichai Shulman, CTO, Imperva

This is due to the lack of fully effective responses, but in some cases, the problem is not one that technology alone can solve. There are numerous elements to the insider threat problem. The following list is a good starting point for organizations looking to control potential insider threat weaknesses:

- Clearly document and consistently enforce policies and controls.
- Incorporate insider threat awareness into periodic security training for all employees.
- Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
- Anticipate and manage negative issues in the work environment.
- Know your assets.
- Implement strict password and account management policies and practices.
- Enforce separation of duties and least privilege.
- Institute stringent access controls and monitoring policies on privileged users.
- Institutionalize system change controls.
- Use a log correlation engine or security information and event management system to log, monitor, and audit employee actions.
- Monitor and control remote access from all end points, including mobile devices.
- Develop a comprehensive employee termination procedure.
- Implement secure backup and recovery processes.
- Develop a formalized insider threat program.

- Establish a baseline of normal network device behavior.
- Be especially vigilant regarding social media.
- Close the door to unauthorized data exfiltration.

By educating your workforce on the signs of potential weaknesses, the insider threat vulnerability can be shrunk significantly.

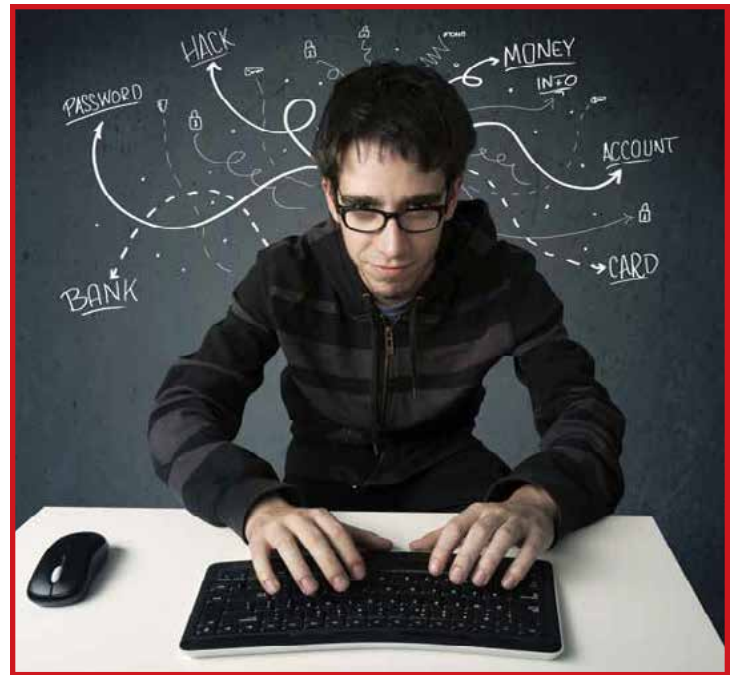
Action Plan

Insider threat is a real and serious problem; never assume that an organization is well protected or immune to insider threats. Insiders, with their authorized access, pose a significant risk. It is vital that organizations have the ability to detect external threats and create systems to protect the organization's information and information systems from unauthorized insider threats.

“Leaks related to national security can put people at risk. They can put men and women in uniform that I’ve sent into the battlefield at risk. They can put some of our intelligence officers, who are in various, dangerous situations that are easily compromised, at risk... So I make no apologies, and I don’t think the American people would expect me as commander in chief not to be concerned about information that might compromise their missions or might get them killed.”

—President Barack Obama

As the cyber domain continues to grow and organizations’ dependency on it expands, the threat vectors associated grow exponentially. It is recommended all organizations be proactive in getting information about insider threats to their workforce, assess their current defenses, and plan actions to improve and increase organizations’ systems. While insider threats can never be completely eradicated,



razstudio/Stock/Thinkstock

a proactive stance can significantly reduce their organizational impact. The threat is real, the problem is complex, but with a layered strategy of policies and procedures, organizational culture, and technical controls, insider threats can be contained.

About the author:

Mr. Greg Smith is the Intelligence Specialist Chief, Intel Division Senior Watch Officer, at the U.S. Coast Guard Cyber Command.

Bibliography:

- Defense Security Service, Counterintelligence Directorate. Insider Threats.
- FBI. *The Insider Threat; An Introduction to Detecting and Detering an Insider Spy*.
- Grimes, R. A., *Insider Threat Deep Dive; Defend Your Network from Rogue Employees*. InfoWorld.
- Information assurance Technology Analysis Center. *The Insider Threat to Information Systems*, October 10, 2006.
- Software Engineering Institute, Carnegie Mellon, *Insider Threat Study: Computer system Sabotage in Critical Infrastructure Sectors*, May 2005.
- Software Engineering Institute, Carnegie Mellon, *Common Sense Guide to Mitigating Insider Threats*, 4th Edition, Dec. 2012.

The Threat Within

Protecting against internal enemies.

by MR. SCOTT O'CONNELL

Former Director

National Geospatial-Intelligence Agency Threat Mitigation Center

What do we mean by “insider threat?” It is a term for the potential danger posed by a disgruntled, malicious, or traitorous employee. Moreover, the threat from such employee(s) can be to other employees, national security, proprietary information, technologies, capabilities, infrastructure, or financial assets.

Most CEOs, directors, and managers will say employees are their most important assets. And, they certainly are. Despite the growth and our reliance on information technology (IT) systems, automated tools, and equipment that seem to permeate and drive today's workplace, success is still ultimately about people. Employees develop our plans, operate our systems, review information, and conceive new approaches.

And, unlike machines and systems, employees have brains, minds, and hearts.

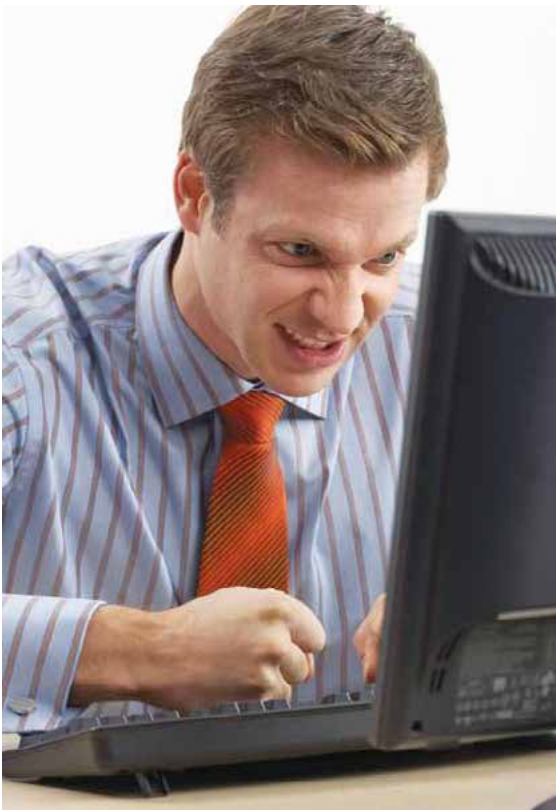
It is the employee that enables a creative work environment that is evolving, productive, and proactive. An engaged workforce is the one that thrives in the workplace, works as a team, and seeks better ways to accomplish individual, team, and organizational goals. However, systems have one advantage over people: They can be secured. Employees are trusted, but not secured. Trust is a difficult thing to measure, and it is even more difficult to guarantee. Even the most trustworthy employees can have something in their lives that causes them to turn toward mischief.

But what if an employee does become a problem or even a potential threat? One employee, intent on mischief, can cause catastrophic damage to an organization's mission, capabilities, and people. Whether someone steals secrets, prototypes of emerging tools, or keys/codes, the results can be immense in time, capital, and capability to replicate what they gave away. Worse, an employee with malicious intent can sabotage systems, equipment, and the physical plant; harm a co-worker; or deny services.

Why is Insider Threat of Concern to the Maritime Domain?

Ships and ports are fragile systems that rely on effective cohesion of crews, equipment, and systems. The impact of just one insider—a crew member gone bad—can be catastrophic. In the port, that can mean loss of time, equipment, or capability to move cargo to and from its intended destination. Sabotage by cyber or kinetic means in peacetime could wreak economic havoc and even disrupt U.S. strategic infrastructure. In wartime, sabotage or espionage could impact military operations as gravely as a major enemy attack.

On a ship, the threat is more acute. For one thing, ships are not just workplaces, but living spaces as well. The ship is your world. Therefore, a malicious attack is an attack on the



Fuse/Thinkstock

The History of Harm

An insider threat is not a new problem: History is replete with examples of trusted insiders who turned against their leaders, organization, tribe, or nation. These weren't always spies. Some were saboteurs or even assassins. For example:

- In Roman times, Gaius Cassius Longinus betrayed his longtime associate, Julius Caesar, enabling the Roman ruler's assassination.
- During the American War for Independence, American General Benedict Arnold gave up the defense plans for West Point to the British. Fortunately, his handler, Major John Andre, was captured and the plot foiled (although Arnold escaped).
- During the early 19th century, the commander of the American Army, General James Wilkinson (a paid agent of Spain), was linked to the Aaron Burr plot to pry the Western U.S. from the East.
- During World War II, a German Luftwaffe officer assigned to the high command proved to be an agent of the Soviet Red Orchestra spy ring. Before detection, he passed critical war plans to his control in Switzerland. Those plans enabled Stalin to avoid certain

destruction on the battlefield and eventually crush Hitler's last assault in the east.

- In early 1972, the aircraft carrier *USS Ranger* was delayed deploying for four months after a Navy fireman dropped a heavy paint scraper into a main reduction gear, destroying one of the engines. Although the Navy could not prove it was intentional, the sabotage was real and affected a wartime deployment.

Possibly the most effective (not a good thing) insider threat was Julius Rosenberg, who provided atomic secrets to the Soviets, unleashing a global nuclear arms race.

Bibliography:

Cole, J. and Carol Symes, Judith Coffin, Robert Stacey. *Western Civilizations: Their History and Their Culture*. Brief Third Edition. Vol. 1, Paperback, September 22, 2011.

John Evangelist Walsh, *The Execution of Major Andre*.

Shreve, R.O. *Finished Scoundrel: General James Wilkinson, Sometime Commander-in-Chief of the Army of the United States, Who Made Intrigue a Trade and Treason a Profession*. Hardcover, January 1, 1933.

V. E. Tarrant, *The Red Orchestra*.

We Are Everywhere: The Movement Grows In The Fleet. See www.sirnosir.com/archives_and_resources/library/articles/up_against_bulkhead_02.html.

Joe Bruno and Lawrence Venturato, *Julius and Ethel Rosenberg—Spies or Scapegoats?*

entire crew and its very existence. It is not a stretch to realize that close and constant living among co-workers brings on all sorts of unique dynamics, some of which can lead to conflict that could result in the desire to get back at one or more members of the crew. This is a risk in all work environments, but ships are particularly closed social and work units that rely on the technical expertise, professionalism, and crew cohesion for effective maritime operations.

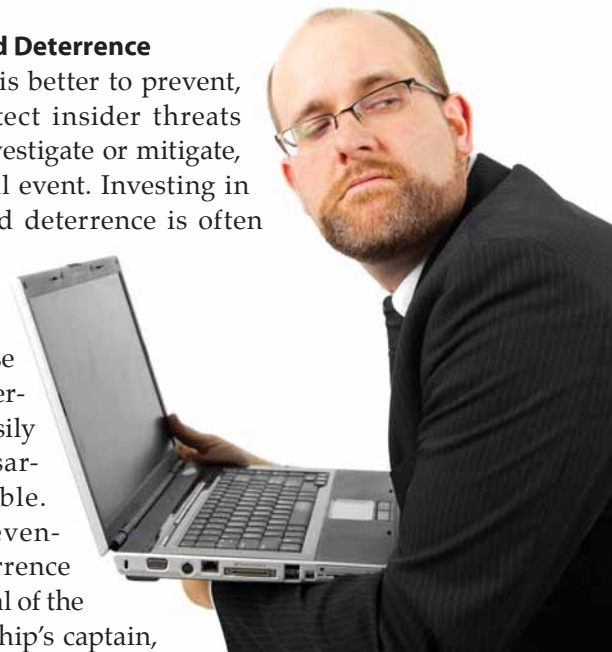
One person acting against the interests of the ship and its crew can cause all manner of harm, including disrupting or destroying mechanisms, power sources, electronics, computers, navigational devices, food, and water. A motivated and trained malicious insider could do enough damage to put the ship out of action, harm the crew, and potentially put the ship at risk of sinking. Malicious action can be subtle, perhaps not even immediately detected. But it can also be so sudden and severe it is not detected until it is too late to undo or reverse the damage.

Insider threat programs are multi-faceted and often include an interlocking array of security and other procedures. Regardless of the extent or form of an insider threat program, someone must be charged with management, integration, and oversight.

Prevention and Deterrence

In all cases, it is better to prevent, deter, and detect insider threats rather than investigate or mitigate, after a harmful event. Investing in prevention and deterrence is often a hard sell to management, because of the cost and because successful deterrence is not easily or even necessarily quantifiable. However, prevention and deterrence must be the goal of the port director, ship's captain, and the management team. Three steps to remember:

- 1 Don't let potential problems into the organization. Have an organization that attracts quality candidates, not just those with impeccable professional credentials, but also ones with backgrounds that are free from obvious problems with regard to suitability.



Pawel Gaul/iStock/Thinkstock

The Long Pole in the Tent

The cyber aspects of an insider threat program are necessarily the most complex and costly, but also the most effective and important component in an age where most employees have access to your network, at least part of the time. The responsibilities in the cyber arena are usually split between those responsible for network security and the element responsible for insider threat detection (normally counterintelligence and/or security).

Decide who is responsible for enterprise audit and continuous monitoring. This restricts and controls activities on the network. Within the maritime domain, this might be as simple as preventing deck or navigational crew from accessing engineering files and systems. Conversely, it might be prudent to prevent engineering crew members from accessing navigational files and systems.

User activity monitoring (also called user behavior monitoring), is distinct and different from enterprise audit and continuous monitoring. It refers to audit data collection strategies that leverage hardware and/or software triggers to detect, monitor, and analyze anomalous user computer behavior for indicators of misuse or insider threat concern. This is normally handled by an organization's counterintelligence element or its security element, if there is no counterintelligence function. In some cases, there could be a distinct insider threat element that performs this function.

2 Have programs and activities aimed at rigorous and continuous vetting. Most insider threats come from employees whose attitudes and predisposition toward the organization change after she or he has worked there for a time.

3 Have programs that allow nuance in background and experience.

Detection

Insider threat awareness and training should be the cornerstone of any program. As employees are an organization's most valuable assets, they are also the first line of defense to detect potential threats from within. More than management, the workforce knows what is going on around it. People sense trouble, they observe it, but they often do not report it—or at least they don't report it to the right person in time to prevent malicious activity. With Americans, it is a cultural thing. We don't like snitches. However, a good awareness program will explain the need and the desirability of reporting suspicious activity or persons, for the good of all.

Insider threat reporting is the next piece. A climate that provides a way for employees to easily and discreetly report suspicious activity 24/7 is essential. An organization's culture should be taken into account. If the culture works primarily

on a computer network, personnel can set up a blind mail box. Some employees might prefer a toll-free telephone number to call in their concerns. Also, supervisors should be trained and made available as a direct reporting channel. However, some might prefer to go directly to "security." If your vessel or the port has a security office, it should certainly be a channel as well.

Cybersecurity is critical if a sizeable portion of the port's workforce or ship's crew has access to the network. For purposes of this discussion, we are concerned with employees who have authorized access to the networks and systems, not hackers from outside. Obviously, such internal cyber threats can be cataclysmic from the standpoint of systems sabotage (including denial of service); theft of critical data or information (not "just" national security data); and theft of goods and services (fraud). Password use, certificates, controlled access, and network audits are some of the tools necessary for success.

Insider threat monitoring and analysis is becoming a more important component of a holistic insider threat program for those entities reliant on computer networks for mission success (that would be most organizations today). There are powerful tools available for all kinds of monitoring, and they must be able to identify anomalous activity. The key here is to understand the rhythm of the organization and its focus on employee behavior (not the employee's background). There are great challenges here regarding data collection, storage, and retrieval. However, once those are overcome, the key then is in quality analysis, for it is analytic judgment, not a computer, which ultimately determines whether an employee's behavior requires further inquiry.

Supply chain risk threats are an often overlooked source of insider threat. An insider can introduce malicious hardware or software to the ship or port with insidious results. There is also a risk posed to the ship from offshore manufacturing processes that can be subverted if not strictly controlled. Once installed, they pose a unique kind of insider threat. To counter this, all hardware and software must be appropriately vetted and the people and processes that acquire or purchase them should be as well.

Technical threats should not be overlooked either. Most people carry around various forms of media that have the

capability to collect all types of data. Most are a type of computer with the potential interface to the network that can bring about denial of service, identity and data theft, and data manipulation. Without physically connecting to the network, an insider can record images, sounds, and even signals to adversely impact a mission.

Data Collection and Analysis

More data is better. Big data analytics offers the potential to break down mass amounts of information to achieve indicators of anomalous behavior, both on and off the network.

Just as the operating systems on a ship or in a port are constantly analyzed to detect potentially harmful anomalies, data concerning a ship's crew or a port's workforce should be gathered and analyzed. What data should be gathered and how it should be analyzed varies with the operating environment and the culture of the organization. Public and private sector may require different rules and protocols.

However, as a minimum, records pertaining to security, human resources, maintenance, computer, logistics, and discipline should be reviewed and analyzed on a continuous basis. In the government, this could extend into financial data, travel information, and workforce and first line supervisor surveys.

You cannot have enough data. To be useful, data needs to be analyzed. Insider threat analysis is not a pick-up game. There needs to be a central analytic capability (even if only one person) devoted to resolving identified concerns. For large organizations with huge amounts of data, teams of analysts armed with proper automated tools are required.

Risk Assessments

Risk assessments can be as simple as a survey, or as complex as an extensive Inspector General or other type of inspection. They are useful for addressing the potential impact of known or postulated threats against ship or port vulnerabilities. The focus may be on analyzing activities, policies, or procedures that could have shortfalls exploitable by an insider who means harm. These are not investigations or even security reviews *per se*. Separate or as part of this, some entity in the organization should be responsible for maintaining an understanding of the types of threats posed to the organization. These can be "cyber" or "bricks and mortar." There are plenty of sources for threat information within government and many available in industry as well through general "open source" reporting or industry-specific sources.

Behavioral Science Support

"Do behave!" said Austin Powers, the international man of mystery who had a global audience rolling with laughter.

But poor employee behavior is no joke. Even the best employee can have a series of life and on-the-job stressors that can lead to a sudden, impulsive, or even well-planned attack on the organization. An insider who turns bad usually does so over a period of time, and personality and behavioral indicators identified early on can help detect and deter malicious activity. Motive, opportunity, ego, lack of inhibition, and lax security all contribute to a hostile insider's decision to act.

Behavioral science support has proven critical to helping an insider threat program identify potential problems on inception, or even prevent them from developing. At the end of the day, the business is people and behavioral science provides a unique perspective on how to categorize behavior in the workplace, assess it, and respond to it. Behavioral science can help inform and even drive a wide variety of insider threat activities, including cyber behavior, personnel security determinations, anomalies analysis, investigations, and training. Behavioral scientists can help you get to the root causes of anomalous and dangerous employee behavior. Also, using the plethora of current and past studies, they can customize these models of such behavior for your organization.

Security Programs

These are still a lynch-pin of any insider threat program, especially in the government. Security checks, criminal records checks, and background investigations backed by sound adjudicative standards provide a modicum of assurance for an employee entering the workforce. Periodic reinvestigations, incident-driven investigations, and continuous monitoring provide a baseline means of assessing employees already in the workforce. Controls on access help assess employee compliance with existing rules and protocols and may help deter or detect a potential threat.

Compliance Actions

When an insider threat is discovered, unlike the proverbial dog that chases a car, organizations or agencies should make sure they know what to do if they catch their quarry. Plans and protocols must be in place for swift, appropriate, and legal action.

The nature of this will vary with the type of threat posed as well as the organization's needs. The threat of physical harm to another employee requires swift action by security or law enforcement. The theft of secrets or proprietary information might require security, counterintelligence, the Inspector General, and possibly law enforcement. But the response might be more deliberative, or not, depending on the specifics.

Each organization should have a “playbook” set up in advance that lays out roles and responsibilities of the stakeholders, based on the nature of the threat. A “tiger team” of cross-functional experts should meet regularly to ensure roles and responsibilities are clearly understood.

Legal and Privacy Considerations

Any insider threat program must have extensive legal review and oversight. Ensure all plans and programs receive a legal opinion. But lawyers should not render such opinions in a vacuum. Those charged with the insider threat mission need to work closely with their counsels to inform them on programs and procedures early on, so everyone can work jointly to ensure legal sufficiency as well as protection from malicious threats. This makes sense on many levels, but especially if a threat comes in the form of criminal activity. It would do no one any good to be unable to prosecute because a sound legal basis for the program was not front-loaded.

Privacy is a growing area of expertise in the government as well as private industry. In today’s information age, management must ensure its employees’ personally identifiable information is protected. Some organizations have appointed privacy officers who are trained and have expertise in how to comply with privacy requirements. Others leave that role to their legal counsel. Either way is fine, as long as those safeguards are incorporated into the organization’s insider threat program.

Deciding What’s Best

Should my organization, port, or vessel have an insider threat program? Perhaps, but it is likely that it already does, albeit not necessarily a formal one. Basic due diligence in hiring and alert supervisors and employees exist in every agency. These provide a seminal alert system for potential problems. But in most modern organizations that might not be enough.

The complexity of the modern workplace, in a port or at sea, makes all too easy for someone who has gone bad to do incalculable damage. A well-crafted insider threat program can go a long way to avoid or limit that damage. And failure to have adequate safeguards can result in a cataclysmic loss of mission, resources, proprietary data, and even people.

For more information:

There are numerous resources available for those trying to build an insider threat program.

National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. Washington, DC: White House Memorandum, November 2012.

Bunn, M. and Scott D. Sagan. *A Worst Practices Guide to Insider Threats: Lessons Learned from Past Mistakes.* American Academy of Arts and Sciences, 2014.

Silowash, G., and Dawn Cappelli, Andrew Moore, Randall Trzeciak, et al (2012). *Common Sense Guide to Mitigating Insider Threats.* Software Engineering Institute, Technical Report, 4th Edition.

Guido, M. D., and Mark W. Brooks. *Insider Threat Program Best Practices.* MITRE Corporation, 2011.

Caputo, D. D. and Greg Stephens, Brad Stephenson, Minna Kimm. *Human behavior, Insider Threat and Awareness.* Institute for Information Infrastructure Protection, July 2009.

Your insider threat program can be simple or complex, depending on your organization’s needs and resources. But it should be tailored to the organization and its mission, functions, and people.

About the author:

Mr. Scott O’Connell served more than 20 years as an Army intelligence officer, mostly in counterintelligence assignments at the operational, command, and staff levels. He was director of Joint Counterintelligence on the JCS staff and director of operations at the Department of Defense Counterintelligence Field Activity. He most recently served as the director of the National Geospatial-Intelligence Agency’s Counterintelligence Threat Mitigation Center.

The Frenemy

Insider threats in the maritime environment.

by COLONEL STEVE COPPINGER (USAF, RET.)
Executive Director (Technical), CACI Inc.

On March 24, 2014, Jeffrey Tyrone Savage drove onto the Norfolk naval shipyard after presenting his properly obtained Transportation Worker Identification Credential at the main gate. He went directly to a pier in an attempt to board the guided missile destroyer, USS *Mahan*. When he approached the ship, he was confronted by ship security personnel. A struggle ensued, and after disarming one of the ship's guards, he used the seized weapon to fatally shoot another sailor. Savage was subsequently killed by other armed personnel on the ship. Navy investigators found no connection between Savage and the ship or anyone on it.¹

In a related insider-threat incident, a Navy network systems administrator formerly assigned to the nuclear reactor department of the aircraft carrier USS *Harry S. Truman* is being prosecuted for leading a computer hacking group called Team Digi7al, which allegedly broke into networks belonging to more than 30 government agencies, private companies, and individuals. The alleged hacker was discharged from the Navy for attacking the Navy's system of arranging the logistics of service member relocations, stealing their personal information, and then posting it online. It cost the Navy in excess of \$500,000 to mitigate the system problem and pay for identify theft protection for all of the victims.²



The U.S. Coast Guard Cutter *Maui* transits alongside the USS *Harry S. Truman*. U.S. Navy photograph by LCDR Steve Mavica, CVN 75 PAO.

These and similar insider threat situations with maritime connections highlight the need for U.S. Coast Guard leaders to establish, organize, and deploy an effective insider threat detection program.

It is important to point out that the term “insider threat” covers a broad range of personality types and motivations. Most importantly, all of these threats have one common dominator: They are individuals who are already “inside” the crew, may be authorized access to the ship or facility, or may be present at associated USCG support facilities. They are already cleared and have access. The question is: “Could they pose a threat to the organization and the crew?”

Fortunately, one of the leading service providers regarding insider threat defense, Kaspersky Labs, has developed an essential listing of the kinds of insider threats (see sidebar).³

The Personality of an Insider Threat

USCG leaders and supervisors must identify and recognize some of the personality traits of an insider threat and consider establishing some potential behavior monitoring capabilities. Deloitte Consulting recently published a report that outlined ways for leaders to understand the psychology behind seemingly disgruntled or disloyal workers.⁴

continued on page 79

Examples of Insider Threats

The careless insider: This is the most common type of insider threat. They are typically negligent, non-supervisory crew members who can cause a breach of operational information, administrative information, or personnel security data. They can cause harm or damage unintentionally, through carelessness or unthinking actions. Careless insiders usually have no real incentive to violate ship or operational security; they are just negligent. Regardless, they can be a real threat to operations.

The naive insider: This describes a person who is vulnerable to being duped—often via social engineering, personal contacts, or other means—to disclose operational, personal, or sensitive information. They don't recognize the risk of revealing information to malicious parties and are particularly vulnerable to approaches by online hackers, foreign intelligence entities, international terrorists, drug cartels, and other criminal elements.

The saboteur: Clearly malicious insiders, saboteurs are personnel who attempt to harm the ship or shipmates for their own personal reasons or special causes that they feel so strong about that they will turn against the organization and its mission. They are often disgruntled, angry, or are subverted by loyalty to special causes such as environmental or political issues. Regardless of their motivations, they are a significant threat to the Coast Guard, its assets, and fellow personnel. Fortunately, these kinds of insiders are not widely present.

The disloyal insider: One of the most harmful insiders over time, the disloyal insider includes personnel who have decided, for various reasons, to provide operational information or classified or

sensitive information to foreign intelligence entities, international terrorist organizations, drug cartels, or other organizations seeking to damage the unit or compromise operational missions. This damage is often not limited to the unit or ship; it can affect the entire Coast Guard, or even the United States. This category includes the spy who decides to commit espionage by providing classified information for personal gain or ideological reasons to unauthorized elements.

The active shooter insider: An extremely dangerous insider, active shooters seem to be on the increase, due to media attention, copy-cats, or other troubling trends. These violent insiders usually have legitimate access to your ship or organization, and have made the decision to hurt or kill as many personnel as possible for their own reasons. These personnel are usually mentally unbalanced but, unfortunately, remain well-organized, motivated, and extremely violent. USCG leaders must have a well-prepared, aggressively exercised action plan for dealing with an active shooter on a ship or in a facility. This includes defensive actions for unarmed personnel (shelter in place), proper emergency response actions (armed), and constant drilling of a response plan for all members of a crew or organization.

The moonlighter: Less present in the USCG environment, the moonlighter is someone who steals USCG or operational information and uses it for their second occupation. This usually means their second job can benefit from inside information about the organization. Such information could include a ship's current mission, targets, location, or capabilities. These types use whatever information they have access to as a

means of generating money or favors in return. Although they may see this type of information leaking as harmless, they have no clear idea who the real end-users or beneficiaries of their sensitive information may be—drug cartels, smugglers, poachers, international terrorists, and such. This category can also include individuals who seek or use inside information for monetary benefit—swinging contracts for kickbacks, providing contract sensitive data to contractors for money, selling USCG material or supplies for personal gain, and such.

The hacker: This category covers USCG personnel who, for various reasons, including ego, will try to access restricted information and databases associated with Coast Guard operational or intelligence activities. These personnel may try to get others to provide passwords, digital identifications, and items that help them access information to which they are not authorized. Some hackers see this as a game. Some may have superiority complexes of such a nature that they are drawn to the challenge of defeating security or access controls.

The leaker: Recently seen in the news, these insiders steal Coast Guard classified or sensitive data and provide it to the mass media or WikiLeaks-like websites. These insiders can compromise USCG classified information or disclose sensitive operational plans and activities. Many of these insiders have political or ideological leanings that drive them to make sensitive USCG operations or capabilities public.

Kaspersky Labs, *Recognizing different types of insiders*, Securelist, <http://securelist.com/threats/recognizing-different-types-of-insiders/>, (2014).

This includes the need for co-workers and supervisors to observe and note certain behaviors, and then report those observations to organizational leaders. USCG leaders and supervisors can be well served by such an “early warning” capability. This includes ensuring your crew is sensitive to behaviors of fellow crewmates that raise suspicion or cause concern.

Dr. Michael Gelles, co-author on the Deloitte report and former chief psychologist for the Naval Criminal Investigative Service, identified some key personality traits of at-risk employees:

- have a history of managing crises inefficiently;
- display a pattern of frustration, disappointment, and inadequacy;
- constantly seek validation;
- have an exaggerated view of their own abilities and achievements;
- a strong sense of entitlement;
- view self above the rules;
- need immediate gratification, validation, and satisfaction.

Gelles went on to note that within organizations, rules are very important to control individuals from becoming a threat to secure and effective operations. He said, “If there aren’t hard-set policies, rules, and the appropriate training, people aren’t going to do things they don’t feel are important... or they’re going to do things because they’re ignorant.”⁵

Commanders and supervisors must also be aware of “generational issues” in relation to insider threats. The Deloitte study also noted that members of Generation Y and younger groups have a tendency to transmit about themselves and their activities. This proclivity, combined with connections to social media, and a passive attitude about information sharing, points to the fact that the incoming federal workforce is already creating its own set of risk factors based on how they typically (and sometimes constantly) use the Internet and communicate with others.

A final list of traits to identify possible insider threats includes the following patterns and precursors.

Insider threat behavior patterns:

- noticeable mood changes,
- increasing negativity,
- attempts to undermine coworkers.



Matt Antonino/Hemera/Thinkstock

External precursors:

- not getting a bonus or promotion,
- workplace dispute,
- personal issue outside of work.

Reporting

DHS

Report all suspicious activity, including cybersecurity incidents, possible malicious code, vulnerabilities, and phishing-related scams.

Call: (888) 282-0870

Email: soc@us-cert.gov

Online: <https://www.us-cert.gov/forms/report>

National Response Center

Report maritime cybersecurity incidents impacting your COTP zone.

Call: (800)-424-8802

Coast Guard Networks

To report a cybersecurity incident impacting applications or systems, contact the Cybersecurity Operations Center.

Call: (202) 372-2900 or (800) 424-2478

Email: CGCYBER-SOC@uscg.mil



Tactical Law Enforcement Team South members participate in a law enforcement active shooter emergency response class. U.S. Coast Guard photo by Petty Officer Michael Anderson.

Combining the elements above with other factors, such as the length of an employee's career, the employee's amount of access to classified data and results of a background check should give leaders and supervisors a fair idea of which employees are most likely to become an insider threat, or even commit an insider attack.

What should leaders do?

The U.S. government, plus various departments and agencies are quickly rolling out mandated insider threat detection and mitigation requirements, especially for organizations with intelligence programs or other sensitive missions.

For commanders and supervisors in a maritime environment, action to counter insider threats is vital. Here are some key steps for preparing the ship and crew to effectively mitigate insider threats:

Preparation: Appoint an experienced staff officer as the insider threat lead, responsible for learning about U.S. government insider threat mandates and policies. This person will be the main source of insider threat detection program (ITDP) updates, new policies, and emerging ITDP tools, techniques, and procedures.

Organize: Get your command in line with current USCG guidelines for an effective ITDP effort. Stopping insider threats is a team effort. It requires all the skills and capabilities of your staff: command element, security, personnel, law enforcement, counterintelligence, legal, medical,

training, and such. Everyone has to be "all in" to protect your mission capabilities from insider threats.

Train and practice: Start a proactive training system. A well-trained staff, capable of recognizing anomalous peer behavior, can greatly enhance security. Some of the simplest programs such as, "If you see something, say something," can mean the difference between an effective intervention or a future active shooter situation. Once personnel have been trained on insider threat detection and effective responses, the organization as a whole must practice those response plans. This is particularly important regarding an insider active shooter. All crew members must know their role, response actions, and specific defensive techniques and procedures in these life-threatening situations.

Communicate: It is vital that senior leaders stress the need for the Coast Guard to look after its own. Personnel who see the value of helping each other will be much more effective in the early identification of others who need assistance. Emphasis on getting any and all personnel help when

needed will set the tone for the entire unit. They will quickly see that identifying those in need and getting them help is a positive and appreciated action.

About the author:

Colonel (ret.) Steve Coppinger, USAF, served as a special agent in the Air Force Office of Special Investigations. He is currently an executive director for CACI Inc., and helps government organizations protect and defend against insider threats.

"What we're not doing here is looking to profile anyone, or point the finger at anyone. What we're trying to do is look for anomalous behaviors. Those are behaviors that begin to look very different than what a person has been normally doing."

—Dr. Michael Gelles, Deloitte Consulting

Endnotes:

- Black, J. *Virginia Truck Driver Shot Sailor at Norfolk Base, Navy Says*. NBC News, March 27, 2014. Available at www.nbcnews.com/news/us-news/virginia-truck-driver-shot-sailor-norfolk-base-navy-says-n64191.
- Ackerman, S. *US sailor shot dead aboard destroyer at Naval Station Norfolk*. The Guardian, March 25, 2014. Available at www.theguardian.com/world/2014/mar/25/naval-station-norfolk-us-sailor-shot-dead.
- Yadron, D. *Navy Systems Administrator Arrested on Hacking Charge*. Dow Jones Business News, May 5, 2014. Available at www.nasdaq.com/article/navy-systems-administrator-arrested-on-hacking-charges-20140505-01561#ixzz317WZguJn.
- Recognizing different types of insiders*. Kaspersky Labs, Securelist, 2014. Available at <https://www.securelist.com/en/threats/internal?chapter=100>.
- Gelles, Dr. M., and Tara Mahoutchian. *Mitigating the Insider Threat — Building a Secure Workforce*. Deloitte Consulting, March 2012. Available at http://csrc.nist.gov/organizations/fissea/2012-conference/presentations/fissea-conference-2012_mahoutchian-and-gelles.pdf.
- Ibid.

Lessons Learned

from USCG Casualty Investigations

In this ongoing feature, we take a close look at recent marine casualties. We outline the U.S. Coast Guard marine casualty investigations that followed, which explore how these incidents occurred, including any environmental, vessel design, or human-error factors that contributed to each event.

Article information, statistics, conclusions, and quotes come from the final, promulgated Coast Guard investigation report.



Into the Storm

Tall ship Bounty founders at sea.

by Ms. Sarah K. Webster
Managing Editor



On Wednesday, October 24, 2012, at 11 a.m., the National Hurricane Center released a “Hurricane Sandy Advisory,” indicating a storm located approximately 65 miles south of Kingston, Jamaica, had turned into a hurricane.

A Plan to Leave Port

On Oct. 25, 2012, as Hurricane Sandy headed northbound toward the Atlantic Coast, the tall ship *Bounty*'s master held a meeting with the crew to inform them of his plan to leave New London, Connecticut, for St. Petersburg, Florida.

The master told his 15-member crew that he had been monitoring the storm and briefly mentioned his plan to deal with it. He wanted to sail out to the east, monitor the hurricane, and then choose what course to take. The master told his crew that he had experience with hurricanes and heavy weather. He believed the ship would be safer out at sea than in port. The master gave the crew an opportunity to stay

behind, if they did not feel comfortable making the trip. He did not, however, inform them of any forecasts, projections, or a description of the storm's projected size, strength, or scope.¹

The master gave his crew less than one hour to make their decisions. If crew members chose to leave, they would have to pay for their own transportation home. (This was standard policy whenever a crew member left the vessel.) No one chose to stay behind,² and so the ship departed port at approximately 6 p.m. The vessel proceeded out to sea, and once it cleared the southern tip of Long Island, it proceeded on a general course of south by southeast, as the master had



Preconditions

When the master departed New London to head toward Hurricane Sandy, he knew the following information:

- The vessel had a history of “making” water through the hull and deck under normal operation and much more so in heavy seas.¹
- The vessel’s age and history.
- The open deficiencies from the ABS 2010 load line examination, most of which involved watertight integrity and watertight subdivision.
- The vessel’s frames and hull planking had decay, but the master did not know to what extent. It was never explored in the shipyard; however, one of the shipyard employees said under testimony that he had warned the master to “pick and choose how he used the boat,” and to avoid heavy weather.
- The weight movements on the vessel during the shipyard period had changed the longitudinal center of gravity and invalidated the vessel’s stability letter. The master did not know how the change in trim and distribution of weight was going to affect the vessel.
- The crew had concerns that the electric bilge dewatering system was not functioning properly. The hydraulic pumps onboard were rarely used, and no one other than the master had experience using them. Moreover, the hydraulic pumps were not tested prior to departure. The gasoline powered trash pump was not tested and no one aboard was familiar with its operation.
- Several crew members were inexperienced. The engineer had less than two weeks underway and was not familiar with the engine room. The cook had been aboard for one day. Also, 10 out of 16 crew members had less than one season experience on the vessel.
- The crew had not completed an abandon ship or fire drill since before the yard period (August 2012).
- He knew there was a hurricane. Company and crew testimony, emails, and text messages all showed conclusively that the master had utter and total clarity on the size, scope, and forecast of Hurricane Sandy. He charted the position of the storm and knew exactly where it was.

Endnote:

1. There are two other separate flooding incidents that are known to the Coast Guard, where the master was in command:
 - a. In October 1998, the vessel was transiting from Massachusetts to St. Petersburg, Florida, when the vessel encountered a storm. The vessel began to take on water when the bilge pumps failed. The vessel was only able to make it to Charleston, South Carolina, with the assistance of the U.S. Coast Guard, a U.S. Navy damage control team, and several other assisting vessels.
 - b. In December 2010, the vessel was transiting from Boothbay Harbor, Maine, to winter berth in Puerto Rico, when the vessel encountered a storm. The vessel began to take on water when the bilge pumps had difficulty keeping up with water ingress. There was damage to the vessel’s masts and rigging, but the vessel was able to make it to Bermuda for an emergency port call. This incident was never reported to the Coast Guard.

planned.³ The crew went into their watch routine and began to stow and secure items to prepare for the hurricane.

Trouble Ahead

On Saturday, Oct. 27, 2012, all forecasts predicted the hurricane to turn to the west and make landfall in New Jersey. However, despite these forecasts, the master chose to alter the vessel’s course from east-southeast to southwest, which placed it into the direct path of the storm, approximately 188 nautical miles from Atlantic City, New Jersey.

Soon after, the weather deteriorated rapidly with swells growing between 15 to 20 feet in size and winds gusting up to 70 knots. By late Saturday morning, the heavy seas were making it difficult to walk about the vessel, and lifelines were rigged on the tween decks to assist crew members. Regardless of the precautions, the engineer fell on deck and fractured his hand.

By evening, the crew grew concerned about the excessive water in the bilges.⁴ The ship had been known to take on

some water during heavy seas, but by the evening the amount of water became atypical. At this time, the vessel’s electric bilge pumps were running continuously, so the master ordered his crew to hook up a hydraulically driven bilge pump and place it in the engine room—the pump would run off of the starboard main engine.

On Sunday morning, Oct. 28, 2012, the seas grew between 20 to 30 feet in size, with winds in excess of 90 knots. The vessel was on a course of 233 degrees true at a speed of 4 knots, motoring under both main engines and sailing under its fore course sail. At this time, the crew started to feel sea sickness and/or fatigue. The engineer fell again, this time in the engine room, and suffered a gash on his arm and injured his leg.

The electric bilge pumps were still in continuous operation, but having difficulty drawing suction, because of the changing water levels. Moreover, the portable hydraulic pump became clogged, due to debris in the bilges.

Around noon, the vessel's port main engine and generator stopped running, when the port day tank ran out of fuel. The vessel's electric bilge pumps now relied on the starboard generator. At approximately 2 p.m., the vessel's sail forward blew out at the seams and had to be furled. Moreover, the electric bilge pumps had trouble maintaining their prime since Saturday, possibly due to the heavy seas causing water in the bilges to move away from the strainers, causing them to suck air. Then at approximately 5 p.m. the starboard generator's power began to fluctuate.

During the night, the crew brought the generators offline several times to replace the fuel filters, which also shut down the electric bilge pumps. With every loss of power, the water level in the bilges grew higher. Moreover, the wind and waves had worsened, causing the vessel to roll more severely, which resulted in more injuries to those aboard including the master. The master fell across the tween deck and hit his back against the table. Also around this time, the fore course⁵ came out of its furl. The crew was unsuccessful in fixing it, so it remained partially unfurled.

Calling for Help

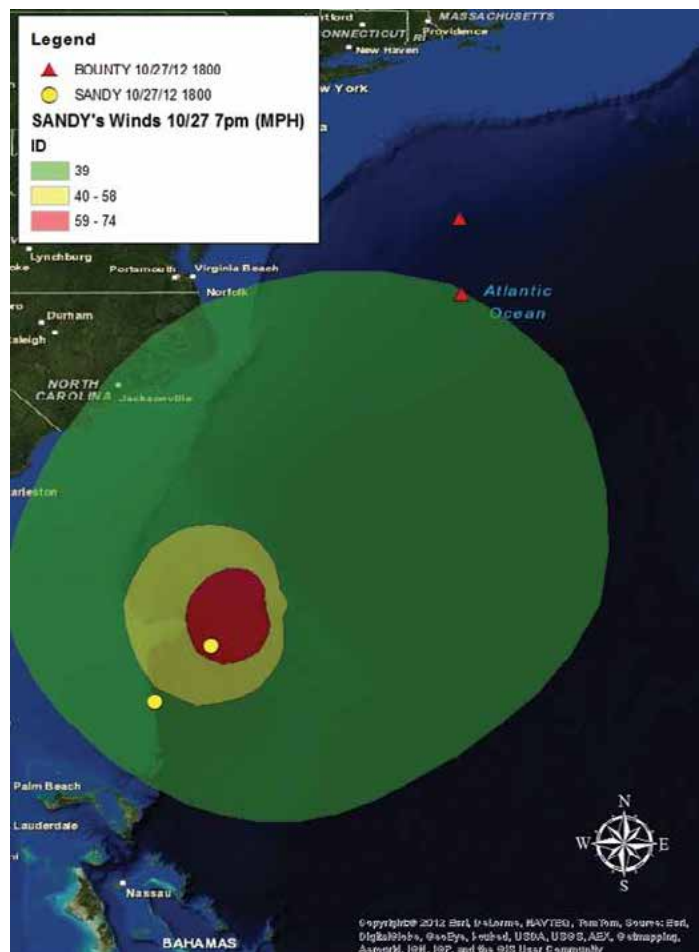
The master and chief mate used a satellite phone and an HF email system to call for assistance. They notified the vessel owner via satellite phone, who directed the vessel's shore support to contact the U.S. Coast Guard. At approximately 8:45 p.m., the vessel's shore support notified the U.S. Coast Guard about the vessel taking on water, approximately 90 miles southeast of Hatteras, North Carolina.

At the same time as the notification from shore support, the Coast Guard received a distress signal from the vessel's Emergency Position-Indicating Radio Beacon. The Coast Guard launched a C-130H to provide over-watch and establish direct communication with the vessel.

At approximately 9:30 p.m., the vessel's starboard generator ceased operating when water from the bilges splashed up and shorted it out. The starboard main engine and the portable hydraulic pump continued to work, but the vessel lost the dewatering battle and began taking on water at about 2 feet per hour. The master directed that an emergency, gasoline-powered bilge pump be put into operation; however, no one could make it work. Later that same night, the second mate got the port generator to work again at approximately 10:30 p.m., which allowed for continued communications with the U.S. Coast Guard.

Abandon Ship!

By Monday morning, Oct. 29, 2012, conditions only got worse. The master directed the crew to prepare to abandon ship and notified the Coast Guard of their intentions to do so. The master wanted to abandon ship at first light to



The tall ship *Bounty* 488 nautical miles from the center of Hurricane Sandy. Used by permission. Copyright © 2013 Esri, DeLorme, NAVTEQ, TomTom, Source: Esri, DigitalGlobe, GeoEye, i-cubed, USDA, USGS, AEX, Getmapping, Aerogrid, IGN, IGP, swisstopo, and the GIS User Community. All rights reserved.

ensure more favorable condition and allow time for Coast Guard assets to arrive.

At approximately 3:30 a.m., the water reached the vessel's tween deck level, so the crew retreated to the weather deck. The crew donned immersion suits and prepared "ditch kits." Less than an hour later, the vessel rolled to starboard on its beam ends.⁶ Although the vessel did not capsize fully, the heeling moment forced the crew to abandon ship without the ditch kits that they had prepared. Most of the crew boarded the two canopied life rafts.

Around 6:30 a.m., two MH- 60 Jayhawks from Elizabeth City arrived on the scene and rescued 14 out of 16 crew members: 13 from the life rafts and one from the open ocean. The Coast Guard returned with the rescued crew to Air Station Elizabeth City. Two crew members received medical attention from local hospitals for injuries, and the rest were debriefed and released to the Red Cross. One crew member and the master remained missing.

The History Behind the Ship

The vessel, constructed for the 1962 film “Mutiny on the Bounty,” was actually a replica of the 1787 Royal Navy sailing ship *HMS BOUNTY*. Although designed for a film, the vessel could perform ocean voyages, much like its predecessor.

After filming the movie, the vessel sailed on a worldwide promotional tour and became a tourist attraction in several locations, but primarily Fall River, Massachusetts, and St. Petersburg, Florida. It also appeared in several other motion pictures.

Under its most current ownership, the vessel operated as a temporarily moored attraction vessel. In this capacity, the vessel moored at a pier or fixed structure, and passengers would embark for tours, after paying a fee. For approximately twenty years prior to the casualty, the Coast Guard primarily inspected the vessel as a moored attraction vessel.

Outside of its regulatory oversight of the vessel’s service as a moored attraction vessel, the Coast Guard treated the vessel as a recreational vessel. A review of the documentary and testimonial evidence indicated that the Coast Guard presumed that when the vessel traveled from port to port, it did so as a recreational vessel. As such, the vessel would have been subject to requirements of 33 CFR Parts 175 and 183. The operating assumption regarding the vessel’s status as a recreational vessel is reflected, among other items, in evidence uncovered by this investigation.

The vessel was not certificated, or permitted, to carry passengers for hire, while underway as a passenger vessel, as defined in 46 U.S.C. § 2101 (22). However, a witness testified that the vessel did carry passengers on occasions, when issued a special permit.

One Recovered from the Sea

The airborne search continued through the morning into Monday afternoon, Oct. 29, 2012. At 4:30 p.m., the Coast Guard found the missing deckhand, unresponsive. The deckhand did not survive. Moreover, the search for the missing master continued and ultimately encompassed approximately 10,000 square miles of search patterns (22 patterns), using surface and air assets. The Coast Guard Fifth District commander suspended the search at approximately 8 p.m., Thursday, Nov. 1, 2012. The master remains missing and is presumed dead. The vessel sank approximately 123 miles southeast of Cape Hatteras, North Carolina, in approximately 14,000 feet of water.

Lessons Learned

The weather was clearly a factor from the beginning of the voyage. Although the conditions related to Hurricane Sandy did not directly affect the vessel until Saturday, Oct. 27,

2012, once the conditions began to worsen, increasing seas accelerated the rate the vessel was taking on water. And the increasing winds blew out multiple sails and caused the spanker gaff to break.

Moreover, the increasing sea state caused many crew members to become seasick, and the conditions also made it difficult to get adequate sleep, not only because of the rough seas, but because the crew sleeping quarters became saturated with water that leaked through the deck. As the voyage progressed and conditions worsened, moving about the vessel became increasingly difficult and resulted in three crew injuries.

Environmental conditions affected the crew’s ability to communicate with one another on deck, as well as communicate with the U.S. Coast Guard, or any other nearby vessels. Environmental conditions also made preparations to abandon ship extremely difficult, for example, donning survival suits, lifejackets, and climbing harnesses.

Once the crew had abandoned ship, the heavy weather conditions made it exceedingly difficult to get into the inflatable life rafts. Crew members testified that entering the life raft took at least one hour once they reached the raft. Wind and seas caused one of the life rafts to flip during the rescue.

The organization failed to provide effective oversight and operating restrictions for its vessel and personnel. The organization’s manager and director, who are both responsible for making critical decisions regarding the maintenance and operation of vessel, were ill equipped to make such decisions due to their lack of experience with vessel operations, especially when considering the uniqueness of an aged, wooden vessel. Also, they each had full knowledge that the master intended to take the vessel into close proximity to Hurricane Sandy, and they took no action to stop this or question the master’s decision making.

The master had the respect of his crew, industry peers, shipyard personnel, and company management. From all reports he had tremendous skill, and he knew the vessel better than anyone. He knew of the vessel’s defects, the magnitude of the storm, and the experience level of his short-handed crew. Therefore, the master should have recognized the very real dangers his decisions imposed on the ship and crew. According to testimony, the chief mate compelled the master to hold a meeting with his crew to address their concerns and convince them that he and the vessel were capable of the trip and that leaving was a way to protect the vessel. However, the master’s actions conflicted with all known maritime methodologies for storm avoidance. Moreover, practically every mariner in the Atlantic chose to either tie up their vessel, or diverted from Hurricane Sandy.

Every tall ship captain interviewed for this investigation indicated disbelief over the actions of the vessel's master and stated they would have never left port, or that they would have sought a safe berth in sufficient time. The master chose to steer toward Hurricane Sandy at a near constant bearing and decreasing range with no compelling reason to do so.

The vessel's only written safety doctrine was the "HMS Bounty Crew Manual." There was no direction or input by the vessel's organization, which meant that the creation, implementation, and execution of risk management efforts were left solely to the master and his crew. With no oversight from the owner or independent outside source, the master instituted a safety culture on the vessel with insufficient standards—especially in the area of voyage planning and emergency operations.

The age of the vessel and the poor condition of its main structure all likely contributed to the vessel taking on water in multiple locations, leading to the progressive flooding. Under normal operating conditions, both underway and at the pier, the vessel relied on its bilge pumps to maintain buoyancy due to the continuous ingress of water through the hull planking. In heavy seas, the frequency and duration of bilge pump "run time" increased, because of the almost exponential increase in water ingress as a result of the hull working during heavy seas. All crew testified to this fact and to the fact that the vessel had a history of near misses related to flooding. The vessel taking on water was apparently an occurrence that was accepted as the norm for wooden vessels. While it is not unusual for wooden hull vessels to make more water in a seaway, a vessel relying primarily on bilge pumps to stay afloat is a sign of more serious defects within the hull structure.

Acknowledgments:

Proceedings would like to thank CDR Kevin Carroll, chief, Prevention Department at Coast Guard Sector Hampton Roads; Mr. Ken Olsen, of the Office of Investigations and Analysis at USCG headquarters; and Mr. Lou Novak, Office of Auxiliary and Boating Safety, Recreational Boating Product Assurance Branch at USCG headquarters, for contributing to this story.



The tall ship *Bounty* is shown submerged in the Atlantic Ocean during Hurricane Sandy, approximately 90 miles southeast of Hatteras, North Carolina, Monday, Oct. 29, 2012. U.S. Coast Guard photo by Petty Officer Tim Kuklewski.

About the author:

Ms. Sarah K. Webster is the managing editor of the *Proceedings of the Marine Safety & Security Council* magazine. She was previously a news reporter and feature writer for *Gannett Inc.*, and a beat reporter for *Micromedia Publications*. She has an M.A. in communication from Kent State University, a B.A. in communication from Monmouth University, and an A.A. in humanities of art from Ocean County College.

Endnotes:

- ¹ Around the same time as the meeting, the National Hurricane Center released another "Hurricane Sandy Advisory," this time listing the storm's current latitude and longitude—placing the storm's center at about 125 miles east southeast of Nassau, Bahamas. The advisory reported "Sandy," as a category two hurricane on the Saffir-Simpson hurricane wind scale. The report indicated that the storm's hurricane winds extended outward to 35 miles and its tropical storm force winds extended outward up to 205 miles. The forecast also addressed the storm's size and indicated the hurricane may grow larger in the following days. The master and the officers had full knowledge of the hurricane's forecasts through Weather Fax, the National Hurricane Center, and television broadcasts.
- ² All crew members interviewed stated that the master's tenure on the ship and his claimed prior history with storms gave them confidence.
- ³ All course information for the vessel analyzed for this investigation was obtained from its Automatic Identification System, with data received by the USCG Navigation Center, Alexandria, Va., and emails from the master.
- ⁴ According to witness testimony, it was typical for the vessel to make water in a heavy seaway.
- ⁵ The sail on a lower mast is called the *course*; thus the sail of the lower mast of the fore mast (the fore lower mast) is called the *fore course*, and the course of the main mast is called the *main course*. See <http://sailing-ships.oktett.net/square-rigging.html>.
- ⁶ A vessel is said to be on her "beam ends" when she is heeled over so far that the deck beams are vertical.

Understanding Dimethyl Sulfide

by CADET NICKOLETTE MORIN
U.S. Coast Guard Academy

What is it?

Dimethyl sulfide is an organic sulfur compound, primarily used as an odorant in natural gas, due to its chemical and thermal stability. It is a colorless to light yellow liquid that produces an unpleasant odor, is insoluble in water, and it can be used as a fuel additive in ethylene oxide to prevent exhaust nozzle fouling and firing chamber carbon deposition. In ethylene manufacture, dimethyl sulfide controls coke and carbon monoxide formation. The natural formation of dimethyl sulfide accounts for 15 percent of global sulfur emissions.

Why Should I Care?

Environmental Concerns:

Dimethyl sulfide is the dominant sulfur compound in the marine environment and a significant part of the global sulfur cycle. Aqueous dimethyl sulfide is converted to its gaseous form in the atmosphere, which is photo-oxidized to sulfur aerosols.

Sulfur aerosol droplets create a positive feedback loop; the droplets scatter solar radiation, creating an “albedo effect,”¹ that results in a higher surface temperature. The higher surface temperatures in turn facilitate dimethyl sulfide production. This process affects Earth’s radiation balance and contributes to global climate change.

Shipping Concerns:

Dimethyl sulfide is considered a Hazard Class 3, flammable and combustible liquid, and is assigned to packing group II, which indicates the degree of danger and dictates packaging, stowage, and segregation requirements. On a vessel, packaged dimethyl sulfide must be stowed away from living quarters.

Health Concerns:

While dimethyl sulfide has an unpleasant odor, it has a low toxicity level. It is flammable in liquid form; therefore, care and the proper protective equipment should be worn when handling dimethyl sulfide liquid. Due to its flammability, dimethyl sulfide can cause temporary incapacitation or residual injury upon exposure.

What is the Coast Guard doing about it?

The Coast Guard enforces maritime transportation requirements for flammable liquids such as dimethyl sulfide. Regulations found in 49 CFR Subchapter C are in place to minimize the risk associated with transporting packaged flammable material.

The United States Coast Guard also operates the National Response Center, the sole federal point of contact for reporting chemical spills. In case of a dimethyl sulfide spill, contact the center at (800) 424-8802.

About the author:

2/c Nickolette Morin is a cadet at the United States Coast Guard Academy studying marine and environmental science. She is interested in a career in response and will graduate in May 2015.

References:

- Airgas. Material Safety Data Sheet: Dimethyl Sulfide.
- Bates, T. *et al.* NOAA. Oceanic Dimethylsulfide and Climate.
- Bo, I.D., J. Heyman, J. Vincke, and H. Van Langenhove. Dimethyl Sulfide Removal from Synthetic Waste Gas Using a Flat Poly(dimethylsiloxane)-Coated Composite Membrane Bioreactor. *Environ. Sci. Technol.*; 2003, Vol. 37, p.p. 4228-4234.
- Smet, E., and H. Van Lagenhove. Abatement of volatile organic sulfur compounds in odorous emissions from the bio-industry. *Biodegradation*; 1998, Vol. 9, p.p. 273-284.
- Norris, K.B. *Dimethylsulfide Emission: Climate Control by Marine Algae?* ProQuest; 2003.
- DMS: Dimethyl Sulfide Overview Bulletin #200B, Gaylord Chemical, 2007.

Endnote:

- ¹. For more information on Albedo effect, see: <https://www.climate.gov/teaching/resources/earths-albedo>.

Nautical Engineering Queries

Prepared by NMC Engineering Examination Team



1. Industrial process and commercial CFC type refrigeration equipment with annual leak rates of 35 percent or more, require leak repair of the system if it contains a refrigerant charge of more than what quantity?

- A. 15 lbs. (6.8 kg)
- B. 25 lbs. (11.4 kg)
- C. 40 lbs. (18.1 kg)
- D. 50 lbs. (22.6 kg)

2. Main condensate recirculating systems are primarily intended to _____.

- A. prevent excessive overheating of the condensate pumps.
- B. balance and control condensate temperatures at full load.
- C. provide adequate cooling water for the air ejector condensers.
- D. vent accumulated vapors from the condensate pump discharge.

3. Fuel combustion in a diesel engine cylinder should begin just before the piston reaches top dead center and should _____.

Note: Fuel combustion commences slightly after fuel injection begins and ends slightly after fuel injection ends. The delay at beginning is called the ignition delay period. The delay at ending is called the after-burning period.

- A. end when fuel injection has been completed
- B. end at bottom dead center
- C. continue through the after-burning period
- D. be completed exactly at top dead center

1. *Note: The mandatory leak repair requirements stipulate that for industrial process and commercial refrigeration CFC type equipment normally containing a refrigerant charge of 50 or more pounds (22.6 kg), leaks must be repaired if the annual leakage rate is 35% or more. These requirements may be found in 40 CFR Part 82.156.*
 - A. 15 lbs. (6.8 kg). Incorrect answer.
 - B. 25 lbs. (11.4 kg). Incorrect answer.
 - C. 40 lbs. (18.1 kg). Incorrect answer.
 - D. 50 lbs. (22.6 kg). **Correct answer. See Note above.**

2. *Note: Main condensate recirculation occurs at very low steam demands, such as while maneuvering, and is triggered by a rise in main condensate temperature.*
 - A. prevent excessive overheating of the condensate pumps. Incorrect answer. Excessive overheating of the condensate pumps is prevented by the main condensate pump casing continuous vent.
 - B. balance and control condensate temperatures at full load. Incorrect answer. Main condensate recirculation occurs at very low steam demands.
 - C. provide adequate cooling water for the air ejector condensers. **Correct answer. At low load, there would be insufficient condensate flow to insure adequate cooling water flow for the air ejector condensers. Condensate recirculation insures adequate cooling water flow.**
 - D. vent accumulated vapors from the condensate pump discharge. Incorrect answer. Venting of accumulated vapors from the condensate pump discharge is accomplished by main condensate pump casing continuous vent.

3. *Note: Fuel combustion commences slightly after fuel injection begins and ends slightly after fuel injection ends. The delay at beginning is called the ignition delay period. The delay at ending is called the after-burning period.*
 - A. end when fuel injection has been completed. Incorrect answer. Fuel continues to burn after injection ends during the after-burning period.
 - B. end at bottom dead center. Incorrect answer. The exhaust valves (or ports) open considerably before bottom dead center, and fuel combustion ends considerably before the exhaust valves (or ports) open.
 - C. continue through the after-burning period. **Correct answer. Fuel continues to burn after injection ends during the after-burning period.**
 - D. be completed exactly at top dead center. Incorrect answer. This is ideally true for a spark-ignition gasoline engine where the fuel burns instantaneously at top dead center, but not for a compression-ignition engine where fuel burns over a comparatively long period of piston travel after top dead center.



Nautical Deck Queries

Prepared by NMC Deck Examination Team

Q

uestions

1. **BOTH INTERNATIONAL & INLAND:** A 50-meter vessel is towing astern and the length of the tow is 100 meters. In addition to sidelights, which lights may the vessel show to fully comply with the rules?
 - A. Two masthead lights forward, a stern light, and a towing light vertically above the stern light
 - B. A masthead light forward, two masthead lights aft, a stern light, and a towing light vertically above the stern light
 - C. No masthead light forward, two masthead lights aft, a stern light, and a towing light vertically above the stern light
 - D. Three masthead lights forward, one masthead light aft, and two towing lights in a vertical line at the stern

2. The cheek length of a block in inches should be about _____.
 - A. Three times the circumference of a manila line.
 - B. Five times the diameter of a manila line.
 - C. Twice the diameter of its sheaves for manila line.
 - D. Twenty times the diameter of a manila line.

3. The “weather adjustment” control on an autopilot steering stand is used to _____.
 - A. allow leeway according to the weather conditions.
 - B. proportionally set the number of degrees of rudder response per degree of course error.
 - C. set the null band or dead zone signal before actuating the rudder.
 - D. set the speed at which the rudder responds.

4. On 20 June your vessel’s 1955 ZT DR position is LAT 52°38.9'N, LONG 03°42.7'E, when an amplitude of the sun is observed. The sun’s center is on the visible horizon and bears 311° per gyrocompass. Variation in the area is 6° W. At the time of the observation, the helmsman noted that he was heading 352° per gyro compass and 358° per steering compass. What is the gyro error and deviation for that heading?
 - A. 1.3° W GE, 1.3° E DEV
 - B. 0.0° GE, 0.0° DEV
 - C. 1.3° W GE, 1.3° W DEV
 - D. 1.3° E GE, 1.3° E DEV

1. A. Two masthead lights forward, a stern light, and a towing light vertically above the stern light. **Incorrect answer.**
 B. A masthead light forward, two masthead lights aft, a stern light, and a towing light vertically above the stern light. **Correct answer.** Reference: International and Inland Rule 23 and Rule 24.
 Rule 23(a) states "a power driven vessel underway shall exhibit: (i) a masthead light forward; (ii) a second masthead light abaft of and higher than the forward one except that a vessel of less than 50 meters in length shall not be obliged to exhibit such light but may do so;"
 Rule 24(a) states "A power driven vessel when towing shall exhibit: (i) instead of the light prescribed in Rule 23(a)(i) or 23(a)(ii), two masthead lights in a vertical line. When the length of the tow measuring from the stern of the towing vessel to the after end of the tow exceeds 200 meters, three such lights in a vertical line; (ii) side-lights; (iii) a stern light; (iv) a towing light in a vertical line above the stern light;"
 C. No masthead light forward, two masthead lights aft, a stern light, and a towing light vertically above the stern light. **Incorrect answer.**
 D. Three masthead lights forward, one masthead light aft, and two towing lights in a vertical line at the stern. **Incorrect answer.**

2. A. Three times the circumference of a manila line. **Correct answer.** Reference: American Merchant Seaman's Manual, Hayler and Kever, Seventh Edition, Page 3-1.
 "The length of a wooden block in inches should be about three times the circumference of the fiber rope to be used with it."
 B. Five times the diameter of a manila line. **Incorrect answer.**
 C. Twice the diameter of its sheaves for manila line. **Incorrect answer.**
 D. Twenty times the diameter of a manila line. **Incorrect answer.**

3. A. allow leeway according to the weather conditions. **Incorrect answer.**
 B. proportionally set the number of degrees of rudder response per degree of course error. **Incorrect answer.**
 C. set the null band or dead zone signal before actuating the rudder. **Correct answer.** Reference: *Electronic Navigation Systems*, Tetley and Calcutt, Third Edition, Page 327.
 D. set the speed at which the rudder responds. **Incorrect answer.**

4. A. 1.3° W GE, 1.3° E DEV. **Incorrect answer.**
 B. 0.0° GE, 0.0° DEV. **Incorrect answer.**
 C. 1.3° W GE, 1.3° W DEV. **Incorrect answer.**
 D. 1.3° E GE, 1.3° E DEV. **Correct answer.** Reference: The American Practical Navigator, Bowditch, 2002 Edition, Page 273 and Table 23.
 Declination is derived from the daily pages of the Nautical Almanac for the GMT of the observation
 Declination = 23° 26.3'N
 $\sin \text{Amp} = (\sin \text{Dec}) / (\cos \text{Lat})$
 $\sin \text{Amp} = (\sin 23.4383^\circ) / (\cos 52.6483^\circ)$
 $\sin \text{Amp} = 0.655608031^\circ$; Amp = 40.9658°
 The amplitude is applied north of west because the sun is setting and the declination is north;
 Amp = 270° + 40.9658°
 Amp = 311° True
 A correction from Bowditch Table 23 is applied to the observed gyro bearing because the body's center is on the visible horizon.
 Table 23 correction = 1.3° Observed gyro bearing = 311°
 Observed gyro bearing = 311° - 1.3° = 309.7°
 Gyro error = the difference between True bearing and Gyro bearing
 Gyro error = 311° - 309.7° = 1.3° East
 True Course = Gyro Course +/- Gyro Error
 True Course = 352° + 1.3° E True Course = 353.3°

| | | | | |
|---------|-----------|----------|-----------|-------|
| Compass | Deviation | Magnetic | Variation | True |
| 358° | 1.3° East | 359.3° | 6° West | 353.3 |

Upcoming in

National Strike Force

21st Century Waterways

Liquefied Gas Carriers and Other Energy Transport

If your command is interested in
"Championing" a *Proceedings* edition,
contact the executive editor at 202-372-2315.
Champion's Guidelines are available on
the *Proceedings* website,
www.uscg.mil/proceedings.

Mailing Address:
U.S. Coast Guard,
Proceedings Magazine,
2703 Martin Luther King Jr. Ave. S.E.
Mail Stop 7318
Washington, DC 20593-7318

Phone:
202-372-2316

Email:
HQS-DG-NMCProceedings@uscg.mil

Website:
www.uscg.mil/proceedings

COMMANDANT (CG-DCO-84)
ATTN: PROCEEDINGS
US COAST GUARD STOP 7318
2703 MARTIN LUTHER KING JR AVE SE
WASHINGTON, DC 20593-7318

PRSRT STD
POSTAGE & FEES PAID
U.S. COAST GUARD
PERMIT NO.G-157

Official Business
Penalty for Private Use, \$300

FORWARDING SERVICE REQUESTED

